JP2002288448 A
LICENSE RECORDER
SANYO ELECTRIC CO LTD
Inventor(s):HORI YOSHIHIRO ;YOSHIKAWA TAKATOSHI
Application No. 2001087395 JP2001087395 JP, Filed 20010326,A1 Published 20021004Published 20021004

Abstract:
PROBLEM TO BE SOLVED: To provide a license recorder which provides a backup of a leased license.
SOLUTION: A memory card 1 is provided with a license area 1415A. The license area 1415A includes licenses (a license ID, a contents ID, a license key Kc, access control information Acm, and reproducing frequency control information Acp), a validity flag, a lease flag, a leased party ID, and license ID at the time of lease. When the license is leased 'under lease' is set to the lease flag, and a public cipher key peculiar to a memory card of the leased party is stored in the leased party ID, and the license ID for lease is stored in the license ID at the time of lease.

Int'l Class: G06F01760; G06K01700 G06K01907
Patents Citing this One: No US, EP, or WO patents/search reports have cited this patent. MicroPatent Reference Number: 000647412

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－288448
（P2002－288448A）
(43)公開日　平成14年10月４日(2002.10.4)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | テーマコード（参考） |
|---|---|---|---|
| Ｇ０６Ｆ　17/60 | ３０２ | Ｇ０６Ｆ　17/60 | ３０２Ｅ　５Ｂ０３５ |
| | ＺＥＣ | | ＺＥＣ　５Ｂ０５８ |
| | １４２ | | １４２ |
| | ５０２ | | ５０２ |
| Ｇ０６Ｋ　17/00 | | Ｇ０６Ｋ　17/00 | Ｌ |

審査請求　未請求　請求項の数９　ＯＬ　（全 44 頁）　最終頁に続く

(21)出願番号　特願2001－87395(P2001－87395)

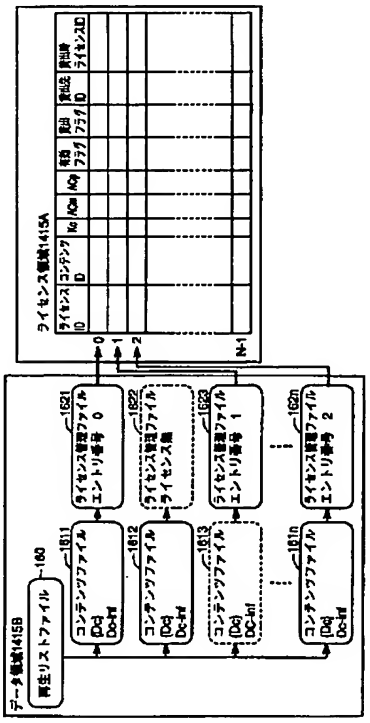
(22)出願日　平成13年３月26日(2001.3.26)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　吉川　隆敏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

Ｆターム(参考)　5B035 AA13 BB09 BC00 CA38
5B058 CA27 KA02 KA04 KA08 KA35
YA20

(54)【発明の名称】　ライセンス記録装置

(57)【要約】
【課題】　貸出したライセンスのバックアップを提供できるライセンス記録装置を提供する。
【解決手段】　メモリカードは、ライセンス領域１４１５Ａを備える。ライセンス領域１４１５Ａは、ライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生回数制御情報ＡＣｐ）、有効フラグ、貸出フラグ、貸出先ＩＤ、および貸出時ライセンスＩＤを含む。ライセンスの貸出が行なわれると、貸出フラグに「貸出中」が設定され、貸出先ＩＤに貸出先のメモリカードに固有な公開暗号鍵が格納され、貸出時ライセンスＩＤに貸出用ライセンスＩＤが格納される。



【特許請求の範囲】
【請求項１】　暗号化コンテンツデータを復号するためのライセンスから貸出用ライセンスを生成し、前記貸出用ライセンスを他のライセンス記録装置へ貸出すライセンス記録装置であって、
前記ライセンスと、前記ライセンスの貸出可否を示す貸出フラグと、前記貸出用ライセンスの貸出先を特定するための貸出先特定情報と、前記貸出用ライセンスを識別するための貸出用ライセンス識別情報とを保持するライセンス保持部と、
制御部とを備え、
前記制御部は、前記ライセンスの貸出要求に応じて、前記他のライセンス記録装置への貸出の対象となるライセンスを指定するためのライセンス指定情報と前記貸出用ライセンスを特定するための貸出用ライセンス特定情報とを外部から受け、前記ライセンス指定情報によって指定されたライセンスを前記ライセンス保持部から読出し、その読出したライセンスに含まれ、かつ、前記読出したライセンスを特定するためのライセンス特定情報を前記貸出用ライセンス特定情報に代えて前記貸出用ライセンスを生成し、前記貸出フラグを貸出中に設定する、ライセンス記録装置。
【請求項２】　前記制御部は、前記ライセンス保持部から読出したライセンスが、複製を禁止され、かつ、移動が許可されたライセンスであるとき、前記貸出用ライセンスを生成する、請求項１に記載のライセンス記録装置。
【請求項３】　前記制御部は、前記貸出フラグが前記ライセンスを貸出していないことを示すとき、前記貸出用ライセンスを生成する、請求項１または請求項２に記載のライセンス記録装置。
【請求項４】　前記制御部は、さらに、前記他のライセンス記録装置における前記貸出用ライセンスの移動および複製を禁止するための制御情報を生成し、前記ライセンス保持部から読出したライセンスに含まれ、かつ、前記読出したライセンスの複製を禁止した制御情報を、前記生成した制御情報に代えて前記貸出用ライセンスを生成する、請求項１から請求項３のいずれか１項に記載のライセンス記録装置。
【請求項５】　前記制御部は、さらに、前記貸出用ライセンス特定情報を前記貸出用ライセンス識別情報として前記ライセンス保持部に格納する、請求項１から請求項４のいずれか１項に記載のライセンス記録装置。
【請求項６】　前記制御部は、さらに、前記他のライセンス記録装置に固有な公開暗号鍵を前記他のライセンス記録装置から受信し、その受信した公開暗号鍵を前記貸出先特定情報として前記ライセンス保持部に格納する、請求項１から請求項５のいずれか１項に記載のライセンス記録装置。
【請求項７】　前記ライセンス保持部は、領域を指定するエントリ番号に対応して前記ライセンス、前記貸出フラグ、前記貸出先特定情報、および前記貸出用ライセンス識別情報を格納しており、
前記制御部は、前記ライセンス指定情報として前記エントリ番号を外部から受ける、請求項１から請求項６のいずれか１項に記載のライセンス記録装置。
【請求項８】　前記ライセンス保持部は、前記貸出先特定情報と前記貸出用ライセンス識別情報とをライセンスの貸出先の数に応じて保持する、請求項１から請求項７のいずれか１項に記載のライセンス記録装置。
【請求項９】　前記ライセンスによって再生される暗号化コンテンツデータを記録するデータ格納部をさらに備える、請求項１から請求項８のいずれか１項に記載のライセンス記録装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを他のライセンス記録装置へ貸出すライセンス記録装置に関するものである。
【０００２】
【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易に情報通信網にアクセスし、情報通信網上のデータを取得することが可能となっている。
【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。
【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の創作物であるコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。
【０００５】一方で、著作権保護の目的を最優先して、急拡大する情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。
【０００６】ここで、上述のような情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体

やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データを情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータの配信においては、パーソナルコンピュータにインストールされたソフトウエアによって暗号化コンテンツデータの配信が行なわれており、暗号化コンテンツデータに対するセキュリティは、暗号化コンテンツデータをメモリカードに書込む場合より低い。また、上記のメモリカードと同じセキュリティを持つデバイスをパーソナルコンピュータに装着すれば、上記の携帯電話機に対する暗号化コンテンツデータの配信と同じ配信をパーソナルコンピュータに対して行なうことが可能である。

【００１５】そうすると、パーソナルコンピュータは、インストールされたソフトウエアと、上記デバイスとによって暗号化コンテンツデータを受信する。つまり、パーソナルコンピュータは、セキュリティレベルの異なる暗号化コンテンツデータを受信する。

【００１６】さらに、音楽データが記録された音楽ＣＤが広く普及しており、この音楽ＣＤから音楽データをリッピングによって取得することも行なわれている。そして、このリッピングによって音楽データから暗号化音楽データ（暗号化コンテンツデータ）と、その暗号化音楽データを復号して再生するためのライセンスとが生成される。そして、このリッピングにおいては、コンテンツデータの利用規則を規定するウォータマークをコンテンツデータから検出し、その検出したウォータマークの内容に応じて暗号化コンテンツデータおよびライセンスが生成される。

【００１７】上述したように、携帯電話機およびパーソナルコンピュータは、配信サーバから暗号化された暗号化コンテンツデータおよびライセンスを受信する。そして、携帯電話機およびパーソナルコンピュータのユーザは、受信した暗号化コンテンツデータおよびライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ移動または複製することもある。この場合、ユーザは、暗号化コンテンツデータを他のユーザの携帯電話機またはパーソナルコンピュータへ移動／複製することは自由でるが、暗号化コンテンツデータを復号するライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ自由に移動することはできない。つまり、ライセンスは、コンテンツ供給者の定めた条件に従って制御され、複製が自由に行なえるライセンス、複製を禁止するものの移動を許可するライセンス、複製・移動をともに禁止するライセンスが存在する。また、音楽ＣＤからのリッピングでは、通常、著作権保護の観点から複製も移動も禁止しておく必要がある。他のユーザの携帯電話機またはパーソナルコンピュータへ移動したとき、暗号化コンテンツデータの著作権保護の観点から送信側と受信側との両方にライセンスを残すことはできない。そこで、ライセンスの移動を行なったとき、送信側のライセンスを消去する。

【００１８】また、移動および複製が禁止されたライセンスに対しては、返却を条件として他のメモリカード等へライセンスを貸出すことが行なわれている。

【００１９】

【発明が解決しようとする課題】しかし、従来のライセンスの貸出においては、貸出したライセンスと貸出元にあるライセンスとを１対１に対応付けて、貸出元において管理することができない。つまり、貸出元において、貸出したライセンスのバックアップを提供することができないという問題があった。

【００２０】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、貸出したライセンスのバックアップを提供できるライセンス記録装置を提供することである。

【００２１】

【課題を解決するための手段】この発明によれば、ライセンス記録装置は、暗号化コンテンツデータを復号するためのライセンスから貸出用ライセンスを生成し、貸出用ライセンスを他のライセンス記録装置へ貸出すライセンス記録装置であって、ライセンスと、ライセンスの貸出可否を示す貸出フラグと、貸出用ライセンスの貸出先を特定するための貸出先特定情報と、貸出用ライセンスを識別するための貸出用ライセンス識別情報とを保持するライセンス保持部と、制御部とを備え、制御部は、ライセンスの貸出要求に応じて、他のライセンス記録装置への貸出の対象となるライセンスを指定するためのライセンス指定情報と貸出用ライセンスを特定するための貸出用ライセンス特定情報とを外部から受け、ライセンス指定情報によって指定されたライセンスをライセンス保持部から読出し、その読出したライセンスに含まれ、かつ、読出したライセンスを特定するためのライセンス特定情報を貸出用ライセンス特定情報に代えて貸出用ライセンスを生成し、貸出フラグを貸出中に設定する。

【００２２】好ましくは、制御部は、ライセンス保持部から読出したライセンスが、複製を禁止され、かつ、移動が許可されたライセンスであるとき、貸出用ライセンスを生成する。

【００２３】好ましくは、制御部は、貸出フラグがライセンスを貸出していないことを示すとき、貸出用ライセンスを生成する。

【００２４】好ましくは、制御部は、さらに、他のライセンス記録装置における貸出用ライセンスの移動および複製を禁止するための制御情報を生成し、ライセンス保持部から読出したライセンスに含まれ、かつ、読出したライセンスの複製を禁止した制御情報を、生成した制御情報に代えて貸出用ライセンスを生成する。

【００２５】好ましくは、制御部は、さらに、貸出用ライセンス特定情報を貸出用ライセンス識別情報としてライセンス保持部に格納する。

【００２６】好ましくは、制御部は、さらに、他のライセンス記録装置に固有な公開暗号鍵を他のライセンス記録装置から受信し、その受信した公開暗号鍵を貸出先特定情報としてライセンス保持部に格納する。

【００２７】好ましくは、ライセンス保持部は、領域を指定するエントリ番号に対応してライセンス、貸出フラグ、貸出先特定情報、および貸出用ライセンス識別情報を格納しており、制御部は、ライセンス指定情報としてエントリ番号を外部から受ける。

【００２８】好ましくは、ライセンス保持部は、貸出先特定情報と貸出用ライセンス識別情報とをライセンスの貸出先の数に応じて保持する。

【００２９】好ましくは、ライセンス記録装置は、ライセンスによって再生される暗号化コンテンツデータを記録するデータ格納部をさらに備える。

【００３０】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００３１】図１は、本発明によるライセンス記録装置が暗号化コンテンツデータを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００３２】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話に装着されたメモリカード１１０に、またはインターネットを介してデジタル音楽データを各パーソナルコンピュータに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００３３】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【００３４】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

【００３５】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００３６】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００３７】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００３８】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００３９】また、図１においては、パーソナルコンピュータ５０は、メモリカード１１０のライセンス管理に関わる機能と同一機能を備えたライセンス管理デバイス（ハードウェア）を備えることで、携帯電話機１００およびメモリカード１１０を用いて受信したのと同じセキュリティレベルの配信を受けることができる。そして、パーソナルコンピュータ５０は、インターネット網３０を介して、暗号化コンテンツデータとライセンスとを配信サーバ１０から受信する。このとき、ライセンスは、配信サーバ１０とライセンス管理デバイスとの間で所定の手順に従った暗号通信路を用いて、直接、ライセンス管理デバイスにおいて受信され、記録される。暗号化コンテンツデータはそのままＨＤＤに記録される。このライセンス管理デバイスは、メモリカード１１０と同じようにライセンスの送受信や管理の機密性をハード的に保持するものであり、機密性が高いものである。

【００４０】さらに、図１においては、パーソナルコンピュータ５０は、ライセンス管理モジュールを使って音楽データを記録した音楽ＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ）６０から取得した音楽データからローカル使用に限定された暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを生成する。この処理をリッピングと呼び、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する行為に相当する。リッピングの詳細については後述する。

【００４１】またさらに、パーソナルコンピュータ５０は、ＵＳＢ（ＵｎｉｖｅｒｓａｌＳｅｒｉａｌ　Ｂｕｓ）ケーブル７０によって携帯電話機１００と接続され、暗号化コンテンツデータおよびライセンスを携帯電話機１００に装着されたメモリカード１１０と送受信することが可能である。

【００４２】更に、図１においては、パーソナルコンピュータ５０は、ハードウェアによって機密性を持つコンテンツ再生回路をパーソナルコンピュータに備えれば暗号化コンテンツデータの再生が可能となる。また、ソフトウェアによるコンテンツ再生であっても、十分な機密性が確保できれば、再生可能となる。パーソナルコンピュータにおける再生についての詳細な説明は、本出願における説明を簡略化するために省略する。

【００４３】したがって、図１に示すデータ配信システムにおいては、パーソナルコンピュータ５０は、インターネット網３０を介して配信サーバ１０から暗号化コンテンツデータとライセンスとを受信するとともに、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する。また、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信するとともに、パーソナルコンピュータ５０が配信サーバ１０または音楽ＣＤ６０から取得した暗号化コンテンツデータおよびライセンスを受信する。携帯電話機１００のユーザは、パーソナルコンピュータ５０を介することによって音楽ＣＤから暗号化コンテンツデータおよびライセンスを取得することが可能となる。

【００４４】さらに、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ５０に待避することが可能となる。

【００４５】図２は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信する機能を有しない再生端末１０２を用いた場合のデータ配信システムを示したものである。図２に示すデータ配信システムにおいては、再生端末１０２に装着されたメモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０または音楽ＣＤ６０から取得した暗号化コンテンツデータおよびライセンスを受信する。このように、パーソナルコンピュータ５０が暗号化コンテンツデータおよびライセンスを取得することによって通信機能のない再生端末１０２のユーザも暗号化コンテンツデータを受信することができるようになる。

【００４６】図１および図２に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するため

のコンテンツデータ保護を実現する構成である。

【００４７】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機またはパーソナルコンピュータとも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００４８】なお、以下の説明においては、配信サーバ１０から、各携帯電話機、各パーソナルコンピュータ等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００４９】図３は、図１および図２に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００５０】まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０より携帯電話またはパーソナルコンピュータのユーザに配布される。

【００５１】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００５２】さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、ライセンスとして、ライセンス鍵Ｋｃ、配信サーバ１０からのライセンス鍵等を特定するための管理コードであるライセンスＩＤが配信サーバ１０と携帯電話機１００との間、または配信サーバ１０とパーソナルコンピュータ５０との間でやり取りされる。また、配信によらないライセンス、すなわち、ローカルでの使用を目的とするライセンスを特定するためにもライセンスＩＤは使用される。配信によるものと、ローカル使用のものとを区別するために、ライセンスＩＤの先頭は“０”で始まるものがローカル使用のライセンスＩＤであり、“０”以外から始まるのものを配信によるライセンスＩＤであるとする。さらに、ライセンスとしては、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤや、コンテンツ供給者側の意向や利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ＡＣｍおよびデータ再生端末における再生に関する制御情報である再生制御情報ＡＣｐ等が存在する。具体的には、アクセス制御情報ＡＣｍはメモリカード、およびライセンス管理デバイスからのライセンスまたはライセンス鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【００５３】以後、コンテンツＩＤとライセンス鍵Ｋｃとライセンス１Ｄとアクセス制御情報ＡＣｍと再生制御情報ＡＣｐとを併せて、ライセンスと総称することとする。

【００５４】また、以降では、簡単化のためアクセス制御情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（１：移動複製可、２：移動のみ可、３：移動複製禁止）の２項目とし、再生制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限（ＵＴＣｔｉｍｅコード）のみを制限するものとする。

【００５５】本発明の実施の形態においては、送信元の記録装置（メモリカード、またはライセンス管理デバイス）から受信先の記録装置へのライセンスの移動／複製において、送信元の記録装置に保持されたライセンスの有効・無効を示す有効フラグの運用を行なう。この有効フラグが有効であるとき、ライセンスをメモリカードから外部へ出すことが可能であることを意味し、有効フラグが無効であるとき、ライセンスをメモリカードから外部へ出すことができないことを意味する。

【００５６】また、送信元の記録装置から受信先の記録装置へのライセンスの貸出／返却において、送信元の記録装置に保持されたライセンスが他の記録装置へ貸出が可能か否かを示す貸出フラグ、ライセンスの貸出先を特定するための情報である貸出先ＩＤ、および貸出したライセンスを識別するための識別情報である貸出時ライセンスＩＤの運用を行なう。

【００５７】図４は、図１および図２に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００５８】コンテンツ再生回路には固有の公開暗号鍵ＫＰｐｙが設けられ、メモリカード、およびライセンス管理デバイスには固有の公開暗号鍵ＫＰｍｗが設けられる。そして、公開暗号鍵ＫＰｐｙおよびＫＰｍｗは、コンテンツ再生回路に固有の秘密復号鍵Ｋｐｙおよびメモリカード、ライセンス管理デバイスに固有の秘密復号鍵

Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００５９】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書としてＣｐｙが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスは、ライセンス取得の禁止対象となる。

【００６０】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式で、メモリカード、およびライセンス管理デバイスのクラス公開暗号鍵およびクラス証明書は認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で出荷時にデータ再生回路、メモリカード、およびライセンス管理デバイスにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは、配信システム全体で共通の公開認証鍵である。

【００６１】また、メモリカード１１０、およびライセンス管理デバイスのデータ処理を管理するための鍵として、メモリカード、およびライセンス管理デバイスという媒体ごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【００６２】メモリカードとの、またはライセンス管理デバイスに対するデータ授受における秘密保持のための暗号鍵として、ライセンスの配信、および再生が行なわれるごとに配信サーバ１０、携帯電話機１００、メモリカード１１０、ライセンス管理デバイスにおいて生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００６３】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生回路もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００６４】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカード、およびライセンス管理デバイスによって全てのセッションにおいてセッションごとに発生し、セッションキーＫｓ３は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００６５】図５は、図１および図２に示した配信サーバ１０の構成を示す概略ブロック図である。

【００６６】配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話やパーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００６７】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカード、およびライセンス管理デバイスから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための２種類の公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａまたはＫＰｂによって復号処理を行なう復号処理部３１２と、配信セッションごとに、セッション鍵Ｋｓ１を発生するセッションキー発生部３１６、セッションキー発生部３

１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００６８】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制御情報ＡＣｍを、復号処理部３２０によって得られたメモリカード、およびライセンス管理デバイスの個別公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【００６９】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００７０】図６は、図１および図２に示したパーソナルコンピュータ５０の構成を説明するための概略ブロック図である。パーソナルコンピュータ５０は、パーソナルコンピュータ５０の各部のデータ授受を行なうためのバスＢＳ２と、パーソナルコンピュータ内を制御すると共に、各種のプログラムを実行するためのコントローラ（ＣＰＵ）５１０と、データバスＢＳ２と、データバスＢＳ２に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク（ＨＤＤ）５３０およびＣＤ－ＲＯＭドライブ５４０と、ユーザからの指示を入力するためのキーボード５６０と、各種の情報を視覚的にユーザに与えるためのディスプレイ５７０とを含む。

【００７１】パーソナルコンピュータ５０は、さらに、暗号化コンテンツデータおよびライセンスを携帯電話機１００等へ通信する際にコントローラ５１０と端子５８０との間でデータの授受を制御するためのＵＳＢインタフェース５５０と、ＵＳＢケーブル７０を接続するための端子５８０と、配信サーバ１０とインターネット網３０を介して通信する際にコントローラ５１０と端子５８５との間でデータの授受を制御するためのモデム５５５と、インターネット網３０と接続するための端子５８５とを含む。

【００７２】コントローラ５１０は、プログラムであるライセンス管理モジュール５１１を実行することでインターネット網３０を介して暗号化コンテンツデータおよびライセンスを配信サーバ１０から取得するために、配信サーバ１０との間でデータの授受を制御するとともに、ＣＤ－ＲＯＭドライブ５４０を介して音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得する際の制御を行なう。さらに、パーソナルコンピュータ５０は、配信サーバ１０からのライセンスの受信を行なう際に配信サーバ１０との間で、またはライセンス管理モジュール５１１からリッピングによるライセンスの受信を行なう際にはライセンス管理モジュール５１１との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス５２０とを含む。

【００７３】図７は、図２に示した再生端末１０２の構成を説明するための概略ブロック図である。

【００７４】再生端末１０２は、再生端末１０２の各部のデータ授受を行なうためのバスＢＳ３と、バスＢＳ３を介して再生端末１０２の動作を制御するためのコントローラ１１０６と、外部からの指示を再生端末１０２に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【００７５】再生端末１０２は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ３との間のデータの授受を制御するためのメモリカードインタフェース１２００と、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを受信する際にバスＢＳ３と端子１１１４との間のデータ授受を制御するためのＵＳＢインタフェース１１１２と、ＵＳＢケーブル７０を接続するための端子１１１４とを含む。

【００７６】再生端末１０２は、さらに、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、再生端末１０２のクラスｙは、ｙ＝１であるとする。

【００７７】再生端末１０２は、さらに、クラス固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ３から受けたデータをＫｐ１によって復号し、メモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【００７８】再生端末１０２は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ３上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化し、バスＢＳ３に出力する暗号化処理部１５０６とを含む。

【００７９】再生端末１０２は、さらに、バスＢＳ３上

のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを出力する復号処理部１５１０と、バスＢＳ３より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０によって復号されたライセンス鍵Ｋｃによって暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号する復号処理部１５１６とを含む。

【００８０】再生端末１０２は、さらに、復号処理部１５１６からの出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【００８１】なお、図７においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路１５５０を構成する。

【００８２】一方、図１に示す携帯電話機１００は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータあるいはライセンスの配信を受信する機能を有するものである。したがって、図１に示す携帯電話機１００の構成は、図７に示す構成において、携帯電話網により無線伝送される信号を受信するためのアンテナと、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部とマイクとスピーカと音声コーデック等の携帯電話機が本来備える機能を設けたものである。

【００８３】携帯電話機１００、再生端末１０２の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００８４】図８は、図１および図２に示すメモリカード１１０の構成を説明するための概略ブロック図である。

【００８５】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、自然数ｗ＝３で表わされるものとする。また、メモリカードを識別する自然数ｘはｘ＝４で表されるものとする。

【００８６】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部１４０２と、クラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

【００８７】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【００８８】メモリカード１１０は、さらに、メモリカードインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータから、クラス秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓｌを接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から公開認証鍵ＫＰａを受けて、バスＢＳ４に与えられるデータから公開認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号化処理部１４０６とを含む。

【００８９】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙもしくはＫＰｍｗによって暗号化してバスＢＳ４に送出する暗号化処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを、復号処理部１４１２で復号された他のメモリカード１１０の個別公開暗号鍵ＫＰｍｃｘ（≠４）で暗号化する暗号処理部１４１７とを含む。

【００９０】メモリカード１１０は、さらに、バスＢＳ４上のデータを個別公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ，コンテンツＩＤ）と、有効フラグと、貸出先ＩＤと、貸出時ライセンスＩＤと、付加情報Ｄｃ－ｉｎｆと、メモリカード１１０内に格納される暗号化コンテンツデータを管理する再生リストファイルと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモ

リによって構成される。また、メモリ１４１５は、ライセンス領域１４１５Ａと、データ領域１４１５Ｂとから成る。ライセンス領域１４１５Ａは、ライセンス、有効フラグ、貸出先ＩＤ、および貸出時ライセンスＩＤを記録するための領域である。データ領域１４１５Ｂは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆ、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストファイルを記録するための領域である。そして、データ領域１４１５Ｂは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【００９１】ライセンス領域１４１５Ａは、ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ，コンテンツＩＤ）、有効フラグ、貸出先ＩＤ、および貸出時ライセンスＩＤを記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンス、有効フラグ、貸出先ＩＤ、および貸出時ライセンスＩＤを格納する。ライセンス等に対してアクセスする場合には、ライセンス等が格納されている、あるいは、ライセンス等を記録したいエントリをエントリ番号によって指定する構成になっている。

【００９２】メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０を含む。

【００９３】なお、ライセンス領域１４１５Ａは、耐タンパモジュール領域に構成される。また、ライセンス領域１４１５Ａとデータ領域１４１５Ｂとは、１つのメモリ１４１５内に構成されている必要はなく、それぞれ、別々に構成されていても良い。さらに、メモリ１４１５は、データ領域１４１５Ｂを伴わないライセンス専用の領域であってもよい。

【００９４】図９は、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０の構成を示す概略ブロック図である。ライセンス管理デバイス５２０は、メモカード１１０におけるデータ領域１４１５Ｂに相当する領域を必要としない点、インタフェース１４２４の機能および端子１４２６の形状が異なるインタフェース５２２４と端子５２２６とを備える点が異なるのみで、基本的にメモリカード１１０と同じ構成から成る。ライセンス管理デバイス５２０の認証データ保持部５２００、Ｋｍｃ保持部５２０２、復号処理部５２０４、暗号処理部５２０６、復号処理部５２０８、暗号処理部５２１０、復号処理部５２１２、ＫＰａ保持部５２１４、ＫＰｍｃ保持部５２１６、暗号処理部５２１７、セッションキー発生部５２１８、コントローラ５２２０、Ｋｍ保持部５２２１、復号処理部５２２２、インタフェース５２２４、端子５２２６、切換スイッチ５２４２，５２４６は、それぞれ、メモリカード１１０の認証データ保持部１４００、Ｋｍｃ保持部１４０２、復号処理部１４０４、暗号処理部１４０６、復号処理部１４０８、暗号処理部１４１０、復号処理部１４１２、ＫＰａ保持部１４１４、ＫＰｍｃ保持部１４１６、暗号処理部１４１７、セッションキー発生部１４１８、コントローラ１４２０、Ｋｍ保持部１４２１、復号処理部１４２２、切換スイッチ１４４２，１４４６と同じである。ただし、認証データ保持部５２００は、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａを保持し、ＫＰｍｃ保持部５２１６は、個別公開暗号鍵ＫＰｍ８を保持し、Ｋｍ保持部５２０２は、クラス秘密復号鍵Ｋｍ７を保持し、Ｋｍｃ保持部５２２１は、個別秘密復号鍵Ｋｍｃ８を保持する。ライセンス管理デバイス５２０のクラスを表す自然数ｗはｗ＝７であり、ライセンス管理デバイス５２０を識別するための自然数ｘはｘ＝８であるとする。

【００９５】ライセンス管理デバイス５２０は、ライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ，コンテンツＩＤ）と、有効フラグと、貸出先ＩＤと、貸出時ライセンスＩＤとを記録するメモリ５２１５を、メモリカード１１０のメモリ１４１５に代えて含む。メモリ５２１５は、ライセンス、有効フラグ、貸出先ＩＤ、および貸出時ライセンスＩＤを記録したライセンス領域５２１５Ａを含む。

【００９６】以下、図１および図２に示すデータ配信システムにおける各セッションの動作について説明する。

【００９７】［配信］図１０および図１１は、図１および図２に示すデータ配信システムのパーソナルコンピュータ５０における暗号化コンテンツデータおよびライセンスの購入時に発生する配信セッションを説明するための第１および第２のフローチャートである。なお、この動作を「配信」と言う。

【００９８】図１０における処理以前に、パーソナルコンピュータ５０のユーザは、配信サーバ１０に対してインターネット網３０を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【００９９】図１０を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐを想定して購入条件ＡＣが入力される。

【０１００】暗号化コンテンツデータの購入条件ＡＣが

入力されると、コントローラ５１０は、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データの出力指示を与える（ステップＳ１０４）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して認証データの送信要求を受信する（ステップＳ１０６）。そして、コントローラ５２２０は、バスＢＳ５を介して認証データ保持部５２００から認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａを読出し、｛ＫＰｍ７／／Ｃｍ７｝ＫＰａをバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ１０８）。

【０１０１】パーソナルコンピュータ５０のコントローラ５１０は、ライセンス管理デバイス５２０からの認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストをモデム５５５およびインターネット網３０を介して配信サーバ１０に対して送信する（ステップＳ１１０）。

【０１０２】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１２）、復号処理部３１２においてライセンス管理デバイス５２０から出力された認証データを公開認証鍵ＫＰａで復号処理を実行する（ステップＳ１１４）。

【０１０３】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１６）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ１１８）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を受理しないで配信セッションを終了する（ステップＳ１６６）。

【０１０４】認証の結果、正当な認証データを持つライセンス管理デバイスを装着したパーソナルコンピュータからのアクセスであることが確認されると、配信サーバ１０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１１８）。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ７によって、暗号化処理部３１８によって暗号化される（ステップＳ１２０）。

【０１０５】配信制御部３１５は、ライセンスＩＤを生成し（ステップＳ１２２）、ライセンスＩＤおよび暗号化されたセッションキーＫｓ１は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０１０６】パーソナルコンピュータ５０が、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ７を受信すると、コントローラ５１０は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ７をメモリカード１１０に入力する（ステップＳ１２６）。そうすると、ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、コントローラ５２２０は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ７を受理する（ステップＳ１２８）。そして、コントローラ５２２０は、バスＢＳ５を介して｛Ｋｓ１｝Ｋｍ７を復号処理部５２２２へ与え、復号処理部５２２２は、Ｋｍ保持部５２２１に保持されるライセンス管理デバイス５２０に固有なクラス秘密復号鍵Ｋｍ３によって復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３０）。

【０１０７】コントローラ５２２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部５２１８に対してライセンス管理デバイス５２０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部５２１８は、セッションキーＫｓ２を生成する（ステップＳ１３２）。

【０１０８】暗号化処理部５２０６は、切換スイッチ５２４２の接点Ｐａを介して復号処理部５２２２より与えられるセッションキーＫｓ１によって、切換スイッチ５２４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、および個別公開暗号鍵ＫＰｍｃ８を１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ８｝Ｋｓ１をバスＢＳ５に出力する。バスＢＳ５に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ８｝Ｋｓ１は、バスＢＳ５からインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０に出力され（ステップＳ１３４）、パーソナルコンピュータ５０から配信サーバ１０に送信される（ステップＳ１３６）。

【０１０９】図１１を参照して、配信サーバ１０は、｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、ライセンス管理デバイス５２０で生成されたセッションキーＫｓ２、およびライセンス管理デバイス５２０に固有の公開暗号鍵ＫＰｍｃ８を受理する（ステップＳ１３８）。

【０１１０】配信制御部３１５は、ステップＳ１１２で取得したコンテンツＩＤに従ってライセンス鍵Ｋｃを情報データベース３０４から取得し（ステップＳ１４０）、ステップＳ１１２で取得したライセンス購入条件のデータＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを決定する（ステップＳ１４２）。

【０１１１】配信制御部３１５は、生成したライセン

ス、すなわち、ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたライセンス管理デバイス５２０に固有の公開暗号鍵ＫＰｍｃ８によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８を生成する（ステップＳ１４４）。そして、暗号化処理部３２８は、暗号化処理部３２６からの暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８を、復号処理部３２０からのセッションキーＫｓ２によって暗号化し、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を出力する。配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２をパーソナルコンピュータ５０へ送信する（ステップＳ１４６）。

【０１１２】パーソナルコンピュータ５０は、送信された暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し、バスＢＳ２を介してライセンス管理デバイス５２０に入力する（ステップＳ１４８）。ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを復号処理部５２１２によって復号する。復号処理部５２１２は、セッションキー発生部５２１８から与えられたセッションキーＫｓ２を用いてバスＢＳ５の受信データを復号し、バスＢＳ５に出力する（ステップＳ１５０）。

【０１１３】この段階で、バスＢＳ５には、Ｋｍｃ保持部５２０２に保持される秘密復号鍵Ｋｍｃ８で復号可能な暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝が出力される（ステップＳ１５０）。

【０１１４】コントローラ５２２０の指示によって、暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８は、復号処理部５２０４において、個別秘密復号鍵Ｋｍｃ８によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ１５２）。

【０１１５】パーソナルコンピュータ５０のコントローラ５１０は、ＨＤＤ５３０から読出したライセンス管理ファイルに基づいて、配信サーバ１０から受信したライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号をバスＢＳ２を介してライセンス管理デバイス５２０へ入力する。そして、コントローラ５１０は、ライセンス管理ファイルのライセンス管理情報を追加更新する（ステップＳ１５４）。

【０１１６】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、ステップＳ１５２において取得したアクセス制御情報ＡＣｍに基づいて、取得したライセンスが貸出可能か否かを判定する（ステップＳ１５６）。アクセス制御情報ＡＣｍは、複製・移動制御情報と再生回数制御情報とから成る。複製・移動制御情報として「１」、「２」、および「３」のいずれかが設定されており、「１」はライセンスの複製・移動不可を意味し、「２」は複製不可・移動可を意味し、「３」は複製・移動禁止を意味する。また、再生回数制御情報としては、０～２５５の値が設定されている。そして、０～２５４の値は、設定された値の回数だけ暗号化コンテンツデータの再生が可能であることを意味し、２５５は、暗号化コンテンツデータを無制限に再生できることを意味する。本発明においては、複製・移動制御情報が「２」に設定され、かつ、再生回数制御情報が「２５５」に設定されているとき、ライセンスを貸出できるものとする。なお、再生回数制御情報が「２５５」に設定されていることは、ライセンスの貸出を可能にするための必須条件である。再生回数制御情報が「０～２５４」に設定されているときは、再生回数に制限があり、貸出元と貸出先とで何回、暗号化コンテンツデータを再生したかを管理するのは困難であるため再生回数が有限のときはライセンスの貸出を禁止し、再生回数が無限の場合に限りライセンスの貸出を可能にしたものである。

【０１１７】そして、コントローラ５２２０は、ライセンスの貸出が可能であれば、メモリ５２１５のライセンス領域５２１５Ａのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する（ステップＳ１５８）。一方、ステップＳ１５６において、ライセンスの貸出が不可と判定されたとき、コントローラ５２２０は、ライセンス領域５２１５Ａのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する（ステップＳ１６０）。

【０１１８】ステップＳ１５８またはステップＳ１６０の後、コントローラ５２２０は、ライセンス領域５２１５Ａのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し（ステップＳ１６２）、ライセンス領域５２１５Ａのエントリ番号によって指定された領域に、ステップＳ１５２において受理したライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐ）を格納する（ステップＳ１６４）。そして、ライセンスの配信動作は終了する（ステップＳ１６６）。

【０１１９】ライセンスの配信動作が終了した後、パーソナルコンピュータ５０のコントローラ５１０は、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信

し、配信サーバ１０は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ１０の配信制御部３１５は、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する。

【０１２０】パーソナルコンピュータ５０は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する。そうすると、コントローラ１１０６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ２を介してＨＤＤ５３０に入力する。また、コントローラ５１０は、ライセンス管理デバイス５２０に格納されたライセンスのエントリ番号と、平文のライセンスＩＤおよびコンテンツＩＤを含む暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に入力する。さらに、コントローラ５１０は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し、全体の処理が終了する。

【０１２１】このようにして、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ７とともに暗号化して送信できた公開暗号鍵ＫＰｍ７が有効であることを確認した上でライセンスを配信することができ、不正なライセンス管理デバイスへのライセンスの配信を禁止することができる。

【０１２２】さらに、配信サーバおよびライセンスかんりデバイス５２０でそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１２３】図１に示すデータ配信システムにおいて携帯電話機１００に装着されたメモリカード１１０に対して、直接、ライセンスを配信する動作も図１０および図１１に示すフローチャートに従って行なわれる。すなわち、上記の説明において、パーソナルコンピュータ５０を携帯電話機１００に代え、ライセンス管理デバイス５２０をメモリカード１１０に代えれば良い。また、図１０のステップＳ１０８においては、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａの代わりに認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａがメモリカード１１０から出力される。その他は、上述したのと同じである。

【０１２４】［リッピング］パーソナルコンピュータ５０のユーザは配信によって暗号化コンテンツデータとライセンスを取得する他に、所有する音楽ＣＤから、音楽データを取得して利用することが可能である。著作権者の権利保護の立場から音楽ＣＤのデジタル複製は自由に行なっても良いものではないが、個人が自己の使用目的のために、著作権保護機能を備えるツールを用いて複製し、音楽を楽しむことは許されている。そこで、ライセンス管理モジュール５１１は、音楽ＣＤから音楽データを取得して、ライセンス管理モジュール５１１にて管理可能な暗号化コンテンツデータとライセンスとを生成するリッピング機能を実現するプログラムも含んでいる。

【０１２５】また、近年の音楽ＣＤには、音楽データ内に、ウォータマークと呼ばれる電子透かしを挿入したものがある。このウォータマークには、著作権者によって利用者における利用の範囲が利用規則として書込まれている。利用規則が書込まれている音楽データからのリッピングでは、著作権保護の点から必ずこの利用規則に従う必要がある。以後、利用規則として、複製条件（複製禁止・複製可能世代・複製可）、複製の有効期間、最大チェックアウト数、編集、再生速度、再生可能な地域のコード、複製に対する再生回数制限、利用可能時間が記載されているとする。また、ウォータマークが検出されない場合、すなわち、利用規則が書込まれていない従来の音楽ＣＤもある。

【０１２６】また、リッピングは、音楽ＣＤから、直接、音楽データを取得する他に、アナログ信号として入力された音楽信号を、デジタル化して音楽データとして取得する場合もある。さらには、データ量を減らすために圧縮符号化された音楽データを入力とすることも可能である。また、さらに、本実施の形態による配信システム以外の、配信システムにて配信されたコンテンツデータを入力として取り込むことも可能である。

【０１２７】図１２および図１３を参照して、音楽データが記録された音楽ＣＤからのリッピングによる暗号化コンテンツデータおよびライセンスの取得について説明する。

【０１２８】図１２は、図６に示すパーソナルコンピュータ５０に含まれるＣＤ－ＲＯＭドライブ５４０がＣＤから読出した音楽データをリッピングするソフトウエアの機能を示す機能ブロック図である。音楽データをリッピングするソフトウエアは、ウォータマーク検出手段５４００と、ウォータマーク判定手段５４０１と、リマーク手段５４０２と、ライセンス発生手段５４０３と、音楽エンコーダ５４０４と、暗号手段５４０５とを備える。

【０１２９】ウォータマーク検出手段５４００は、音楽ＣＤから取得した音楽データからウォータマークを検出し、記載されている利用規則を抽出する。ウォータマーク判定手段５４０１は、ウォータマーク検出手段５４０

０の検出結果、すなわち、ウォータマークが検出できたか否か、さらに検出できた場合には、ウォータマークで記載されていた利用規則に基づいて、リッピングの可否を判定する。この場合、リッピング可の場合、ウォータマークの利用規則が無い、または音楽ＣＤに記録された音楽データの複製および移動が許可された利用規則がウォータマークによって記録されていたことを意味し、リッピング不可の場合、音楽ＣＤに記録された音楽データを複製および移動してはいけない利用規則がウォータマークによって記録されていたことを意味する。

【０１３０】リマーク手段５４０２は、ウォータマーク判定手段５４０１における判定結果がリッピング可能で、複製世代の指示がある場合、つまり、音楽データを複製・移動して良い場合、音楽データに含まれるウォータマークを音楽データの複製条件を変更したウォータマークに付け替える。ただし、アナログ信号を入力してリッピングする場合や符号化された音楽データを入力とする場合、および他の配信システムにて配信された音楽データを入力とする場合には、リッピング可能であれば利用規則の内容に関わらず、必ず、ウォータマークを付け替える。この場合、複製世代の指示がある場合は、利用規則の内容を変更して、それ以外の場合には取得した利用規則をそのまま利用する。

【０１３１】ライセンス発生手段５４０３は、ウォータマーク判定手段５４０１の判定結果に基づいてライセンスを発生させる。音楽エンコーダ５４０４は、リマーク手段５４０２によってウォータマークがリマークされた音楽データを所定の方式に符号化する。暗号手段５４０５は、音楽エンコーダ５４０４からの音楽データをライセンス発生手段５４０３により発生されたライセンスに含まれるライセンス鍵Ｋｃによって暗号化する。

【０１３２】図１３を参照して、パーソナルコンピュータ５０のコントローラ５１０におけるリッピング動作について説明する。リッピング動作が開始されると、ウォータマーク検出手段５４００は、音楽ＣＤから検出したデータに基づいてウォータマークの利用規則を検出する（ステップＳ８００）。そして、ウォータマーク判定手段５４０１は、ウォータマーク検出手段５４００の検出結果とウォータマークとして記録されていた利用規則に基づいて複製が可能か否かを判定する（ステップＳ８０２）。ウォータマークが検出され、利用規則によって複製が許可され、かつ、利用規則の内容がライセンス内のアクセス制御情報や再生制御情報にて対応可能な場合、リッピング可と判断され、ステップＳ８０４へ移行する。また、ウォータマークが検出され、利用規則によって複製の禁止、または、ライセンス内のアクセス制御情報や再生制御情報にて対応不可の利用規則が記載されている場合、リッピング禁止と判断され、ステップＳ８２８へ移行してリッピング動作は終了する。装着されたＣＤにウォータマークが含まれていない場合、ステップＳ８１０へ移行する。

【０１３３】ステップＳ８０２において、リッピング可と判断した場合、音楽ＣＤから音楽データが取込まれ、リマーク手段５４０２によって音楽データに含まれるウォータマークが複製条件を変更したウォータマークに付け替えられる（ステップＳ８０６）。すなわち、ウォータマークの利用規則が３世代までの複製を許可している場合、複製世代を２回にしたウォータマークに付け替える。そして、ライセンス発生手段５４０３は、利用規則を反映したライセンスを生成する。すなわち、ライセンス発生手段５４０３は、複製回数が２世代であるライセンスを生成する（ステップＳ８０６）。

【０１３４】一方、ステップＳ８０２において、ウォータマークが検出されない場合、ライセンス発生手段５４０３は、ライセンスの複製のみを禁止した移動・複製制御情報が「２」のライセンスを生成する（ステップＳ８１０）。

【０１３５】ステップＳ８０６またはＳ８１０の後、音楽エンコーダ５４０４は、ウォータマークがリマークされた音楽データを所定の方式に符号化してコンテンツデータＤｃを生成する（ステップＳ８１４）。そして、暗号手段５４０５は、音楽エンコーダ５４０４からの音楽データをライセンス発生手段５４０３により発生されたライセンスに含まれるライセンス鍵Ｋｃによって暗号化を行ない、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを生成する（ステップＳ８１６）。その後、音楽ＣＤに含まれる情報またはパーソナルコンピュータ５０のキーボード５６０から入力されたユーザ入力等によってコンテンツデータ｛Ｄｃ｝の付加情報Ｄｃ－ｉｎｆが生成される（ステップＳ８１８）。

【０１３６】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得し、ＨＤＤ５３０に記録する（ステップＳ８２０）。そして、コントローラ５１０は、生成されたライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生制御情報ＡＣｐ）をライセンス管理デバイス５２０に格納する（ステップＳ８２２）。ライセンス管理デバイス５２０へのライセンスの格納は、コントローラ５１０上で実行されているライセンス管理モジュール５１１を介して図１０および図１１に示すフローチャートのステップＳ１０４からステップＳ１６６に従って行なわれる。すなわち、暗号化コンテンツデータおよびライセンスの配信における説明において配信サーバ１０をコントローラ５１０に代えればよく、コントローラ５１０上で動作中のライセンス管理モジュール５１１は、配信サーバ１０におけるライセンスの配信に対応する機能を実現できるプログラムである。その後、コントローラ５１０は、平文のトランザクションＩＤおよびコンテンツＩＤを含み、か

つ、ＨＤＤに記録した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、ＨＤＤ５３０に記録する（ステップＳ８２４）。最後に、コントローラ５１０は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツのファイル名を追記して（ステップＳ８２６）、リッピング動作が終了する（ステップＳ８２８）。

【０１３７】このように音楽ＣＤからリッピングによっても暗号化コンテンツデータとライセンスとを取得でき、取得されたライセンスは、配信サーバ１０から配信されたコンテンツとともに保護されて管理される。

【０１３８】このように、音楽ＣＤからリッピングによって取得された暗号化コンテンツデータおよびライセンスは、ライセンス管理モジュール５１１によって生成され、配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスと同じように管理される。したがって、パーソナルコンピュータ５０は、音楽ＣＤからリッピングによって取得した暗号化コンテンツデータおよびライセンスを、後述するチェックアウトによって携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ送信可能である。これによって、携帯電話機１００または再生端末１０２のユーザは、パーソナルコンピュータ５０がリッピングによって取得した暗号化コンテンツデータを自己のメモリカード１１０に受信して再生を楽しむことができる。

【０１３９】上記においては、パーソナルコンピュータ５０は、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得したが、本発明においては、これに限らず、他のインターネット配信によって受信したコンテンツデータからリッピングによって暗号化コンテンツデータおよびライセンスを生成しても良い。

【０１４０】［移動］上述したように、メモリカード１１０およびライセンス管理デバイス５２０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを取得できる。そこで、メモリカード１１０またはライセンス管理デバイス５２０が配信サーバ１０から受信したライセンスを他のメモリカードへ移動するときの動作について説明する。

【０１４１】図１４および図１５は、図１および図２に示すデータ配信システムにおいて、ライセンス管理デバイス５２０が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ移動する動作を説明するための第１および第２のフローチャートである。携帯電話機１００または再生端末１０２は、移動においては、データの中継を行なうのみの機器であるため、フローチャートから省略してある。移動を説明するに当たり、図１の携帯電話機１００に装着されたメモリカード１１０へ移動する場合について説明を行なうが、図２の再生端末１０２に装着されたメモリカード１１０へ移動する場合についても同様であり、携帯電話機１００を再生端末１０２に読替えれば良い。また、メモリカード１１０からライセンス管理デバイス５２０へ移動する場合も同様に、ライセンス管理デバイス５２０とメモリカード１１０とを読替えればよい。

【０１４２】なお、図１４における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。また、コントローラ５１０は、ライセンス管理ファイルを保持していることを前提としている。

【０１４３】図１４を参照して、パーソナルコンピュータ５０のキーボード５６０から移動リクエストが入力されると（ステップＳ３００）、コントローラ５１０は、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して認証データの送信要求をメモリカード１１０へ送信する（ステップＳ３０２）。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ３０４）。

【０１４４】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して外部へ出力する（ステップＳ３０６）。そして、パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ３０８）。

【０１４５】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６およびインタフェース５２２４を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ５を介して復号処理部５２０８へ与える。そして、復号処理部５２０８は、ＫＰａ保持部５２１４からの認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ３１０）。コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗

号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ３１２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ３１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ３７４）。

【０１４６】認証の結果、正当な認証データを持つメモリカードであることが確認されると、ライセンス管理デバイス５２０において、コントローラ５２２０は、セッションキー発生部５２１８を制御し、セッションキー発生部５２１８は、移動のためのセッションキーＫｓ２ａを生成する（ステップＳ３１４）。セッションキーＫｓ２ａは、復号処理部５２０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部５２１０によって暗号化される。そして、コントローラ５２２０は、バスＢＳ５を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を取得し、バスＢＳ５、インタフェース５２２４および端子５２２６を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を出力する（ステップＳ３１６）。

【０１４７】コントローラ５１０は、バスＢＳ２を介して｛Ｋｓ２ａ｝Ｋｍ３をライセンス管理デバイス５２０から受理し（ステップＳ３１８）、ＨＤＤ５３０に記録されているライセンス管理情報からライセンスＩＤを取得する（ステップＳ３２０）。そして、コントローラ５１０は、取得したライセンスＩＤと、ステップＳ３１８において受理した暗号化データ｛Ｋｓ２ａ｝Ｋｍ３とを１つのデータにしてライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３を端子５８０およびＵＳＢインタフェース５５０を介して携帯電話機１００に装着されたメモリカード１１０へ送信する（ステップＳ３２２）。そうすると、メモリカード１１０のコントローラ１１０６は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介してライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３を受理する（ステップＳ３２４）。その後、コントローラ１４２０は、暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２ａ｝Ｋｍ３を復号してセッションキーＫｓ２ａを受理する（ステップＳ３２６）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２ｂを生成し（ステップＳ３２８）、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２ｂ、および個別公開暗号鍵ＫＰｍｃ４を、復号処理部１４０４によって復号されたセッションキーＫｓ２ａによって暗号化し、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して出力し（ステップＳ３３０）、パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受理する。そして、コントローラ５１０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをバスＢＳ２を介してライセンス管理デバイス５２０へ送信する（ステップＳ３３２）。

【０１４８】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受信し、その受信した暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号処理部５２１２に与える。復号処理部５２１２は、セッションキー発生部５２１８からのセッションキーＫｓ２ａによって暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号し、セッションキーＫｓ２ｂ、および公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ３３４）。

【０１４９】その後、コントローラ５１０は、ライセンス管理デバイス５２０に対応するライセンス管理情報から移動の対象となっているライセンスが格納されているエントリ番号を取得し（ステップＳ３３６）、その取得したエントリ番号とライセンスの移動要求とをライセンス管理デバイス５２０へ入力する（ステップＳ３３８）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリ番号とライセンスの移動要求とを受信し、その受信したエントリ番号によって指定されるメモリ５２１５のライセンス領域５２１５Ａのエントリからライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）を取得する（ステップＳ３４０）。

【０１５０】図１５を参照して、コントローラ５２２０は、ステップＳ３４０において取得したライセンスの貸出の有無を貸出フラグによって判定する（ステップＳ３４２）。そして、取得したライセンスが貸出中であれば、移動動作は終了する（ステップＳ３７４）。取得したライセンスが貸出中でなければ、コントローラ５２２０は、次いで、アクセス制御情報ＡＣｍを確認する（ステップＳ３４４）。つまり、コントローラ５２２０は、取得したアクセス制御情報ＡＣｍに基づいて、最初に、メモリカード１１０へ移動しようとするライセンスが再生回数によって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数が残っていない場合（再生回数＝０）、暗号化コンテンツデータをライセンスによって再生することができ

ず、その暗号化コンテンツデータとライセンスとをメモリカード１１０へ移動する意味がないからである。再生することができない場合、再生することができる場合、移動・複製制御情報によって、ライセンスの複製、移動の可否を判断する。

【０１５１】ステップＳ３４４において、暗号化コンテンツデータの再生回数ができない（再生回数＝０）、または、移動・複製フラグが移動複製禁止（＝０）の場合、アクセス制御情報ＡＣｍによって、複製移動不可と判断し、ステップＳ３７４へ移行し、移動動作は終了する。ステップＳ３４４において、暗号化コンテンツデータの再生ができ（再生回数≠０）、かつ、移動・複製制御情報が移動のみ可「＝２」の場合、ライセンスの移動であると判断され、コントローラ５２２０は、メモリ５２１５のライセンス領域５２１５Ａにおいて指定されたエントリ番号内の有効フラグを無効する（ステップＳ３４６）。また、暗号化コンテンツデータの再生ができ「再生回数≠０」、かつ、移動・複製制御情報が複製可の場合、ライセンスの複製であると判断され、ステップＳ３４６を行なわずにステップＳ３４８へ移行する。

【０１５２】ステップＳ３４４またはステップＳ３４６の後、暗号化処理部５２１７は、復号処理部５２１２によって得られたメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ３４８）。このように、ライセンスの移動が可能なときは、ライセンス領域５２１５Ａの有効フラグを無効にしてから（ステップＳ３４６参照）、ステップＳ３４８の処理を行なうが、ライセンスの複製が許可されている場合は、複製元と複製先との両方においてライセンスを使用可能にするためにライセンスの有効フラグを無効にするステップＳ３４６を介さずにステップＳ３４８へ移行するようにしたものである。したがって、ライセンスを移動させたときは、ライセンス管理デバイス５２０からライセンスを読出すことはできない。

【０１５３】そして、暗号化処理部５２０６は、暗号化処理部５２１７によって暗号化された暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をスイッチ５２４６の接点Ｐｃを介して受取り、復号処理部５２１２によって復号されたセッションキーＫｓ２ｂをスイッチ５２４２の接点Ｐｂを介して受取り、暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２ｂによって暗号化する。そして、コントローラ５２２０は、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをバスＢＳ５、インタフェース５２２４、および端子５２２６を介して出力する（ステップＳ３５０）。

【０１５４】コントローラ５１０は、バスＢＳ２を介してメモリカード１２０から暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを受理し、その受理した暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをメモリカード１１０へ送信する（ステップＳ３５２）。

【０１５５】メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂの入力を受けて、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを復号処理部１４１２へ与える。そして、復号処理部１４１２は、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２ｂによって復号し、｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ３５４）。

【０１５６】その後、コントローラ１４２０の指示によって、暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ３５６）。

【０１５７】そうすると、コントローラ５１０は、受信側であるメモリカード１１０のライセンス管理情報から移動／複製されたライセンスを格納するためのエントリ番号を決定し、メモリカード１１０に入力するとともに、受信側（メモリカード１１０）のライセンス管理情報を更新する（ステップＳ３５８）。

【０１５８】そうすると、メモリカード１００のコントローラ１４２０は、ステップＳ３５６において取得したアクセス制御情報ＡＣｍに基づいて、取得したライセンスが貸出可能か否かを判定する（ステップＳ３６０）。そして、コントローラ１４２０は、ライセンスの貸出が可能であれば、メモリ１４１５のライセンス領域１４１５Ａのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する（ステップＳ３６２）。一方、ステップＳ３６０において、ライセンスの貸出が不可と判定されたとき、コントローラ１４２０は、ライセンス領域１４１５Ａのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する（ステップＳ３６４）。

【０１５９】ステップＳ３６２またはステップＳ３６４の後、コントローラ１４２０は、ライセンス領域１４１

５Ａのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し（ステップＳ３６６）、ライセンス領域１４１５Ａのエントリ番号によって指定された領域に、ステップＳ３５６において受理したライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐ）を格納する（ステップＳ３６８）。

【０１６０】一方、ステップＳ３５８の後、コントローラ５１０は、ライセンスの移動または複製が可能か否かを判定し（ステップＳ３７０）、移動可能であるとき、送信側のライセンス管理情報、すなわち、移動したライセンスに対応するＨＤＤ５３０に記録されているライセンス管理情報を削除し、送信側のライセンス管理情報およびメモリカード１１０のデータ領域１４１５Ｂに記録されているライセンス管理ファイルを書換える（ステップＳ３７２）。ステップＳ３７０において、ライセンスの貸出が可能と判定されたとき、またはステップＳ３７２の後、またはステップＳ３６８の後、ライセンスの移動動作は終了する（ステップＳ３７４）。

【０１６１】なお、暗号化コンテンツデータのメモリカード１２０からメモリカード１１０への移動は、ライセンスの移動が終了した後、メモリカード１２０のデータ領域１４１５Ｂから暗号化コンテンツデータを読出してメモリカード１１０へ送信することによって行なえば良い。

【０１６２】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、正規なメモリカードへの移動要求に対してのみライセンスを移動することができ、不正なメモリカードへの移動を禁止することができる。

【０１６３】また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動の動作におけるセキュリティを向上させることができる。

【０１６４】また、メモリカード１１０からライセンス管理デバイス５２０へのライセンスの移動も、図１４および図１５に示すフローチャートに従って行なわれる。つまり、図１において、携帯電話機１００によって配信を受け、メモリカード１１０に格納した暗号化コンテンツデータとライセンスとをパーソナルコンピュータ５０へ退避できることになる。

【０１６５】また、パーソナルコンピュータ５０が配信サーバ１０から受信したライセンスをメモリカード１１０へ移動できるのは、ライセンス管理デバイス５２０が配信サーバ１０からハード的に受信したライセンスだけであり、音楽ＣＤからライセンス管理モジュール５１１によってリッピングされたライセンスは移動できない。そこで、次に説明するチェックアウト（貸出）およびチェックイン（返却）の概念によって、ライセンス管理モジュール５１１によってリッピングし、ライセンス管理デバイス５２０に記録したライセンスをメモリカード１１０へ送信できるようにした。

【０１６６】また、メモリカード１２０からメモリカード１１０へのライセンスの貸出、および返却も可能である。「移動」と「貸出」との相違は、「移動」は、ライセンスを移動させた送信元のメモリカードにおいては、ライセンスの有効フラグが無効に設定されている（図１５のステップＳ３４６参照）ため、「移動」は、送信元のメモリカードから暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータの再生を行なうことができないが、「貸出」は、ライセンスを貸出した貸出元のメモリカードから暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータの再生を行なうことができる点にある。また、上述したように、音楽ＣＤからリッピングしたライセンスを送る。

【０１６７】［貸出］図１および図２に示すデータ配信システムにおいて、配信サーバ１０からライセンス管理デバイス５２０へ配信された、あるいは音楽ＣＤからリッピングされた暗号化コンテンツデータおよびライセンスをメモリカード１１０に返却を前提として貸出すために送信する動作について説明する。なお、この動作を「貸出」という。

【０１６８】図１６および図１７は、ライセンス管理デバイス５２０からメモリカード１１０へのライセンスの貸出を説明するための第１および第２のフローチャートである。

【０１６９】なお、図１６における処理以前に、携帯電話機１００のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。また、コントローラ４０は、ライセンス管理ファイルを保持していることを前提としている。

【０１７０】図１６を参照して、パーソナルコンピュータ５０のキーボード５６０から貸出リクエストが入力されると（ステップＳ４００）、コントローラ５１０は、携帯電話機１００を介して認証データの送信要求をメモリカード１１０へ送信する（ステップＳ４０２）。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ４０４）。

【０１７１】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を

介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して外部へ出力する（ステップＳ４０６）。そして、パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ４０８）。

【０１７２】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６およびインタフェース５２２４を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ５を介して復号処理部５２０８へ与える。そして、復号処理部５２０８は、ＫＰａ保持部５２１４からの認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ４１０）。コントローラ１４２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ４１２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ４１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ４７８）。

【０１７３】認証の結果、正当な認証データを持つメモリカードからのアクセスであることが確認されると、ライセンス管理デバイス５２０において、コントローラ５２２０は、セッションキー発生部５２１８を制御し、セッションキー発生部５２１８は、貸出のためのセッションキーＫｓ２ａを生成する（ステップＳ４１４）。セッションキーＫｓ２ａは、復号処理部５２０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部５２１０によって暗号化される。そして、コントローラ５２２０は、バスＢＳ５を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を取得し、バスＢＳ５、インタフェース５２２４および端子５２２６を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を出力する（ステップＳ４１６）。

【０１７４】コントローラ５１０は、バスＢＳ２を介して｛Ｋｓ２ａ｝Ｋｍ３を送信側から受理し（ステップＳ４１８）、送信側のライセンス管理情報、すなわち、ＨＤＤ５３０に記録されている貸出を行なうライセンスに対応するライセンスＩＤを取得する（ステップＳ４２０）。そして、コントローラ５１０は、取得したライセンスＩＤと、ステップＳ４１８において受理した暗号化データ｛Ｋｓ２ａ｝Ｋｍ３とを１つにデータにしてライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３を端子５８０およびＵＳＢインタフェース５５０を介してメモリカード１１０へ送信する（ステップＳ４２２）。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介してライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３を受理する（ステップＳ４２４）。その後、コントローラ１４２０は、暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２ａ｝Ｋｍ３を復号してセッションキーＫｓ２ａを受理する（ステップＳ４２６）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２ｂを生成し（ステップＳ４２８）、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２ｂ、および個別公開暗号鍵ＫＰｍｃ４を、復号処理部１４０４によって復号されたセッションキーＫｓ２ａによって暗号化し、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して出力し（ステップＳ４３０）、コントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受理する。そして、コントローラ５１０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをバスＢＳ２を介してライセンス管理デバイス５２０へ入力する（ステップＳ４３２）。

【０１７５】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受信し、その受信した暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号処理部５２１２に与える。復号処理部５２１２は、セッションキー発生部５２１８からのセッションキーＫｓ２ａによって暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号し、セッションキーＫｓ２ｂ、および公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ４３４）。

【０１７６】その後、コントローラ５１０は、貸出を行なうライセンスに対応したライセンス管理情報から移動の対象となっているライセンスが格納されているエントリ番号を取得し（ステップＳ４３６）、貸出用ライセンスＩＤを生成し（ステップＳ４３８）、ステップＳ４３６において取得したエントリ番号とステップＳ４３８において生成した貸出用ライセンスＩＤとによって指定さ

れたライセンスの貸出要求をライセンス管理デバイス５２０へ入力する（ステップＳ４４０）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリ番号、貸出用ライセンスＩＤ、およびライセンスの貸出要求とを受信し、その受信したエントリ番号によって指定されるメモリ１４１５のライセンス領域５２１５Ａのエントリからライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）を取得する（ステップＳ４４２）。

【０１７７】コントローラ５２２０は、取得したアクセス制御ＡＣｍによってライセンスの複製が可能か否かを判定し（ステップＳ４４４）、複製可であれば図１７のステップＳ４５２へ移行し、複製が禁止されていれば図１７のステップＳ４４６へ移行する。

【０１７８】図１７を参照して、ステップＳ４４４においてライセンスの複製が禁止されていると判定されたとき、ステップＳ４４２において取得したライセンスの貸出可否を貸出フラグによって判定する（ステップＳ４４６）。そして、取得したライセンスが貸出不可であれば、貸出動作は終了する（ステップＳ４７８）。取得したライセンスが貸出可でなければ、コントローラ５２２０は、指定されたエントリ内の貸出フラグを「貸出中」に変更し、受理した貸出用ライセンスＩＤを貸出時ライセンスＩＤの欄に格納し、ステップＳ４３４において受理した公開暗号鍵ＫＰｍｃ４を貸出先ＩＤの欄に格納する（ステップＳ４４８）。そして、コントローラ５２２０は、移動・複製禁止を設定した（移動・複製制御情報が「３」である）貸出用アクセス制御情報ＡＣｍを生成し、受理した貸出用ライセンスＩＤと生成した貸出用アクセス制御情報ＡＣｍとを、指定されたエントリから取得したライセンスＩＤおよびアクセス制御情報ＡＣｍと置換する（ステップＳ４５０）。これによって、メモリカード１１０へ貸出されるライセンス（貸出用ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、貸出用アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）が生成されるとともに、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ａには、元のライセンス（貸出用ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、貸出用アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）が格納されたままである。そして、ライセンス管理デバイス５２０のライセンス領域５２１５Ａに格納されたままのライセンスは、メモリカード１１０へ貸出される。このため、ライセンス管理デバイス５２０には、移動の場合と異なりライセンスが残るためライセンスのバックアップとして機能する。

【０１７９】ステップＳ４４４において複製可と判定されたとき、またはステップＳ４５０の後、暗号化処理部５２１７は、復号処理部５２１２によって得られたメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ４５２）。なお、ステップＳ４４４においてライセンスの複製が可能と判定されたとき、ステップＳ４４２において取得されたライセンスが公開暗号鍵ＫＰｍｃ４によって暗号化される。

【０１８０】そして、暗号化処理部５２０６は、暗号化処理部５２１７によって暗号化された暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をスイッチ５２４６の接点Ｐｃを介して受取り、復号処理部５２１２によって復号されたセッションキーＫｓ２ｂをスイッチ５２４２の接点Ｐｂを介して受取り、暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２ｂによって暗号化する。そして、コントローラ５２２０は、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをバスＢＳ５、インタフェース５２２４、および端子５２２６を介して出力する（ステップＳ４５４）。

【０１８１】コントローラ５１０は、バスＢＳ２を介してメモリカード１２０から暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを受理し、その受理した暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを携帯電話機１００に装着された貸出先のメモリカード１１０へ入力する（ステップＳ４５６）。

【０１８２】メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂの入力を受けて、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを復号処理部１４１２へ与える。そして、復号処理部１４１２は、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２ｂによって復号し、｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ４５８）。

【０１８３】その後、コントローラ１４２０の指示によって、暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ４６

０）。

【０１８４】そうすると、コントローラ５１０は、受信側であるメモリカード１１０のライセンス管理情報から移動／複製されたライセンスを格納するためのエントリ番号を決定し、メモリカード１１０に入力するとともに、受信側のライセンス管理情報を更新する（ステップＳ４６２）。

【０１８５】そうすると、メモリカード１００のコントローラ１４２０は、ステップＳ４６０において取得したアクセス制御情報ＡＣｍに基づいて、取得したライセンスが貸出可能か否かを判定する（ステップＳ４６４）。そして、コントローラ１４２０は、ライセンスの貸出が可能であれば、メモリ１４１５のライセンス領域１４１５Ａのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する（ステップＳ４６６）。一方、ステップＳ３６０において、ライセンスの貸出が不可と判定されたとき、コントローラ１４２０は、ライセンス領域１４１５Ａのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する（ステップＳ４６８）。貸出においては、ステップＳ４５０においてアクセス制御情報の移動・複製制御情報が移動・複製不可に設定されてライセンス管理デバイス５２０から出力されるため必ずステップＳ４６８へ進む。

【０１８６】ステップＳ４６６またはステップＳ４６８の後、コントローラ１４２０は、ライセンス領域１４１５Ａのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し（ステップＳ４７０）、ライセンス領域１４１５Ａのエントリ番号によって指定された領域に、ステップＳ４６０において受理したライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐ）を格納する（ステップＳ４７２）。

【０１８７】一方、ステップＳ４６２の後、コントローラ５１０は、ライセンスの移動または複製が可能か否かを判定し（ステップＳ４７４）、移動可能であるとき、貸出先のライセンス管理情報に貸出用ライセンスＩＤを追記し、貸出先ライセンス管理情報を更新する（ステップＳ４７６）。ステップＳ４７４において、ライセンスの貸出が可能と判定されたとき、またはステップＳ４７６の後、またはステップＳ４７２の後、ライセンスの貸出動作は終了する（ステップＳ４７８）。

【０１８８】なお、暗号化コンテンツデータのメモリカード１１０への貸出は、ライセンスの移動が終了した後、コントローラ５１０がＨＤＤ５３０から暗号化コンテンツデータを読出してメモリカード１１０へ送信することによって行なえば良い。

【０１８９】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、正規なメモリカードへの貸出要求に対してのみライセンスを貸出を行なうことができ、不正なメモリカードへの貸出を禁止することができる。

【０１９０】また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの貸出動作におけるセキュリティを向上させることができる。

【０１９１】［返却］図１６および図１７を参照して説明したライセンス管理デバイス５２０からメモリカード１１０へ貸出されたライセンスをメモリカード１１０からライセンス管理デバイス５２０へ返却する動作について説明する。

【０１９２】図１８～図２１は、メモリカード１１０からライセンス管理デバイス５２０へライセンスを返却する動作を説明するための第１～第４のフローチャートである。

【０１９３】なお、図１８における処理以前に、ユーザは、パーソナルコンピュータ５０にＵＳＢケーブル７０によって接続された携帯電話機１００に装着されたメモリカード１１０から返却されるライセンスおよびコンテンツをＨＤＤ５３０に記録されているコンテンツリストファイルに従って決定し、返却側のコンテンツファイルと貸出側および返却側の双方のライセンス管理ファイルとが特定できていることを前提として説明する。

【０１９４】図１８を参照して、パーソナルコンピュータ５０のキーボード５６０から返却リクエストが入力されると（ステップＳ５００）、コントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データの送信要求をメモリカード１１０へ送信する（ステップＳ５０２）。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ５０４）。

【０１９５】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介してコントローラ５１０へ出力する（ステップＳ５０６）。そして、コントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ５０８）。

【０１９６】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６およびイン

タフェース５２２４を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ５を介して復号処理部５２０８へ与える。そして、復号処理部５２０８は、ＫＰａ保持部５２１４からの認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ５１０）。コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ５１２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ５１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ６３８）。

【０１９７】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであることが確認されると、ライセンス管理デバイス５２０において、コントローラ５２２０は、セッションキー発生部５２１８を制御し、セッションキー発生部５２１８は、返却のためのセッションキーＫｓ２ａを生成する（ステップＳ５１４）。セッションキーＫｓ２ａは、復号処理部５２０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部１４１０によって暗号化される。そして、コントローラ５２２０は、バスＢＳ５を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を取得し、バスＢＳ５、インタフェース５２２４および端子５２２６を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を出力する（ステップＳ５１６）。

【０１９８】コントローラ５１０は、バスＢＳ２を介して｛Ｋｓ２ａ｝Ｋｍ３をライセンス管理デバイス５２０から受理し（ステップＳ５１８）、貸出元のライセンス管理情報から貸出時のライセンスＩＤを取得する（ステップＳ５２０）。そして、コントローラ４０は、取得したライセンスＩＤと、ステップＳ５１８において受理した暗号化データ｛Ｋｓ２ａ｝Ｋｍ３とを１つにデータにしてライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３をメモリカード１１０へ送信する（ステップＳ５２２）。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介してライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３を受理する（ステップＳ５２４）。その後、コントローラ１４２０は、暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２ａ｝Ｋｍ３を復号してセッションキーＫｓ２ａを受理する（ステップＳ５２６）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２ｂを生成し（ステップＳ５２８）、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２ｂ、および個別公開暗号鍵ＫＰｍｃ４を、復号処理部１４０４によって復号されたセッションキーＫｓ２ａによって暗号化し、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して出力し（ステップＳ５３０）、コントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受理する。そして、コントローラ５１０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをバスＢＳ２を介してライセンス管理デバイス５２０へ送信する（ステップＳ５３２）。

【０１９９】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受信し、その受信した暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号処理部５２１２に与える。復号処理部５２１２は、セッションキー発生部５２１８からのセッションキーＫｓ２ａによって暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号し、セッションキーＫｓ２ｂ、および公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ５３４）。

【０２００】そして、コントローラ５１０は、ライセンスの検索要求を貸出先のメモリカード１１０へ入力する（ステップＳ５３４）。メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してライセンスの検索要求を受理し（ステップＳ５３６）、ステップＳ５２４において受理したライセンスＩＤに基づいてメモリ１４１５のライセンス領域１４１５Ａを検索する。そして、コントローラ１４２０は、検索結果ｓｔａｔｅを生成する（ステップＳ５３８）。

【０２０１】暗号化処理部１４０６は、復号処理部１４１２によって復号して得られたセッションキーＫｓ２ａをスイッチ１４４２の接点Ｐｂを介して受け、セッションキー発生部１４１８が発生したセッションキーＫｓ２ｂをスイッチ１４４６の接点Ｐｄを介して受ける。そして、暗号化処理部１４０６は、セッションキーＫｓ２ｂをセッションキーＫｓ２ａによって暗号化して暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを生成する（ステップＳ５４０）。そして、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅを生成し、

その生成したライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅのハッシュ値ｈａｓｈを求める（ステップＳ５４２）。つまり、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅの署名を行なう。その後、コントローラ１４２０は、ハッシュ値ｈａｓｈをスイッチ１４４６の接点Ｐｆを介して暗号化処理部１４０６へ与える。暗号化処理部１４０６は、ハッシュ値ｈａｓｈをセッションキーＫｓ２ａによって暗号化し、暗号化データ｛ｈａｓｈ｝Ｋｓ２ａを生成する（ステップＳ５４４）。

【０２０２】図１９を参照して、メモリカード１１０のコントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａを生成し、バスＢＳ４、インタフェース１４２４、および端子１４２６を介してライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａを出力する（ステップＳ５４６）。コントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介してメモリカード１１０からライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａを受信する（ステップＳ５４８）。そして、コントローラ５１０は、貸出元のライセンス管理情報から返却するライセンスが格納されているエントリ番号を取得し（ステップＳ５５０）、ステップＳ５４８において取得したライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａとエントリ番号を指定したライセンス返却要求とを貸出元のライセンス管理デバイス５２０へ入力する（ステップＳ５５２）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介してライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａとエントリ番号とライセンス返却要求とを受理し（ステップＳ５５４）、その受理したエントリ番号によって指定された領域に格納されている貸出フラグ、貸出時のライセンスＩＤ、および貸出先ＩＤに格納された公開暗号鍵ＫＰｍｃｘを取得する（ステップＳ５５６）。

【０２０３】そうすると、コントローラ５２２０は、取得した公開暗号鍵ＫＰｍｃｘがステップＳ５３４において受理したメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４に一致するか否かを判定し（ステップＳ５５８）、不一致であるとき、返却動作は終了する（ステップＳ６３８）。つまり、メモリカード１１０がライセンスを貸出した相手でないと判定されたことになるので、返却動作を終了することにしたものである。公開暗号鍵ＫＰｍｃｘが公開暗号鍵ＫＰｍｃ４に一致したとき、コントローラ５２２０は、貸出フラグが貸出中になっているか否かを判定し（ステップＳ５６０）、貸出中でなければライセンスを返却する必要がないので、返却動作は終了する（ステップＳ６３８）。ステップＳ５６０においてライセンスが返却中であると判定されると、コントローラ５２２０は、受理したライセンスＩＤが貸出時のライセンスＩＤに一致するか否かを判定し（ステップＳ５６２）、不一致であるとき、返却動作は終了する（ステップＳ６３８）。つまり、返却要求のあったライセンスのライセンスＩＤが貸出したライセンスのライセンスＩＤに一致せず、貸出したライセンスが返却されないことになるので、返却動作を終了することにしたものである。ステップＳ５６２において、２つのライセンスＩＤが一致したとき、コントローラ５２２０は、メモリカード１１０におけるライセンスの検索結果ｓｔａｔｅを確認する（ステップＳ５６４）。すなわち、コントローラ５２２０は、返却しようとするライセンスがメモリカード１１０のライセンス領域１４１５Ａに本当に格納されているか否かを確認し、ライセンス領域１４１５Ａに格納されていないとき、返却動作を終了する（ステップＳ６３８）。そして、コントローラ５２２０は、返却しようとするライセンスがメモリカード１１０のライセンス領域１４１５Ａに格納されていることを確認したとき、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅのハッシュ値ｈａｓｈを求める（ステップＳ５６６）。つまり、ライセンス管理デバイス５２０のコントローラ５２２０は、自らライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅに対する署名を行ない、ハッシュ値ｈａｓｈを求める。

【０２０４】その後、コントローラ５２２０は、ステップＳ５５４において受理した｛ｈａｓｈ｝Ｋｓ２ａを復号処理部５２１２に与える。復号処理部５２１２は、｛ｈａｓｈ｝Ｋｓ２ａをセッションキーＫｓ２ａによって復号し、コントローラ５２２０は、メモリカード１１０におけるハッシュ値ｈａｓｈを受理する（ステップＳ５６８）。そして、コントローラ５２２０は、自ら求めたハッシュ値ｈａｓｈがメモリカード１１０におけるハッシュ値ｈａｓｈに一致するか否かを判定し（ステップＳ５７０）、不一致であるとき、メモリカード１１０における署名が書換えられていることになるので返却動作は終了する（ステップＳ６３８）。２つのハッシュ値が一致したとき、コントローラ５２２０は、ステップＳ５５４において受理した暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを復号処理部５２１２に与える。復号処理部５２１２は、暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａをセッションキーＫｓ２ａによって復号してセッションキーＫｓ２ｂを受理する（ステップＳ５７２）。

【０２０５】そして、コントローラ５２２０は、セッションキーＫｓ２ｂの確認を行ない（ステップＳ５７４）、ライセンスの貸出時にメモリカード１１０から受信したセッションキーＫｓ２ｂと不一致であれば返却動作は終了し（ステップＳ６３８）、一致すれば図２０のステップＳ５７６へ移行する。

【０２０６】図２０を参照して、貸出先に貸出したライ

センスを無効にするための無効ダミーライセンス（偽ライセンスＩＤ、偽コンテンツＩＤ、偽ライセンス鍵Ｋｃ、偽アクセス制御情報ＡＣｍ、および偽再生制御情報ＡＣｐを生成し、その生成した無効ダミーライセンスを暗号化処理部５２１７に与える。暗号化処理部５２１７は、無効ダミーライセンスを復号処理部５２１２によって復号された公開暗号鍵ＫＰｍｃ４によって暗号化し、暗号化データ｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ５７６）。そして、暗号化処理部５２０６は、暗号化データ｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４をスイッチ５２４６の接点Ｐｃを介して受取り、その受取った暗号化データ｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４をスイッチ５２４６の接点Ｐｄを介して受取ったセッションキーＫｓ２ｂによって暗号化して暗号化データ｛｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを出力する。そして、コントローラ５２２０は、バスＢＳ５、インタフェース５２２４、および端子５２２６を介して暗号化データ｛｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを出力する（ステップＳ５７８）。

【０２０７】コントローラ５１０は、バスＢＳ２を介して暗号化データ｛｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを貸出元であるライセンス管理デバイス５２０から受け、貸出先であるメモリカード１１０へ暗号化データ｛｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを送信する（ステップＳ５８０）。

【０２０８】メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを受理し、その受理した暗号化データを復号処理部１４１２に与える。復号処理部１４１２は、暗号化データをセッションキーＫｓ２ｂによって復号して｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ５８２）。そして、復号処理部１４０４は、復号処理部１４１２からの暗号化データ｛偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ｝Ｋｍｃ４をＫｍｃ保持部１４０２からの秘密鍵Ｋｍｃ４によって復号して無効ダミーライセンス（偽ライセンスＩＤ／／偽コンテンツＩＤ／／偽ライセンス鍵Ｋｃ／／偽アクセス制御情報ＡＣｍ／／偽再生制御情報ＡＣｐ）を受理する（ステップＳ５８４）。

【０２０９】そうすると、コントローラ５１０は、貸出先であるメモリカード１１０のライセンス管理情報から返却するライセンスが格納されているエントリ番号を取得し、その取得したエントリ番号を貸出先に送信する（ステップＳ５８６）。メモリカード１１０のコントローラ１４２０は、偽アクセス制御ＡＣｍによってライセンスの貸出が可能か否かを判定し（ステップＳ５８８）、貸出可であればライセンス領域の貸出フラグを「可」に設定し（ステップＳ５９０）、貸出不可であれば貸出フラグを「不可」に設定する（ステップＳ５９２）。ステップＳ５９０またはステップＳ５９２の後、コントローラ１４２０は、エントリ番号によって指定されたライセンス領域１４１５Ａの有効フラグを「有効」に設定し（ステップＳ６９４）、エントリ番号によって指定された領域にライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報、および再生回数制御情報）を格納する（ステップＳ５９６）。ステップＳ５８８，Ｓ５９０，Ｓ５９２，Ｓ５９４，Ｓ５９６の処理は、上述した「配信」および「移動」と共通としているため、処理されるものの偽アクセス制御情報ＡＣｍは、常に移動複製禁止であるためステップＳ５８８においては必ず「貸出不可」と判断され、ステップＳ５９２に進む。

【０２１０】その後、コントローラ５１０は、ライセンスの検索要求を貸出先に再び入力し（ステップＳ５９８）、メモリカード１１０のコントローラ１４２０は、ライセンスの検索結果を端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して受理する（ステップＳ６００）。コントローラ１４２０は、ライセンスＩＤに基づいてメモリ１４１５のライセンス領域１４１５Ａを検索する。そして、コントローラ１４２０は、検索結果ｓｔａｔｅを生成する（ステップＳ６０２）。

【０２１１】暗号化処理部１４０６は、復号処理部１４１２によって復号して得られたセッションキーＫｓ２ａをスイッチ１４４２の接点Ｐｂを介して受け、セッションキー発生部１４１８が発生したセッションキーＫｓ２ｂをスイッチ１４４６の接点Ｐｄを介して受ける。そして、暗号化処理部１４０６は、セッションキーＫｓ２ｂをセッションキーＫｓ２ａによって暗号化して暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを生成する（ステップＳ６０４）。そして、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅを生成し、

その生成したライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅのハッシュ値ｈａｓｈを求める（ステップＳ６０６）。つまり、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅの署名を行なう。その後、コントローラ１４２０は、ハッシュ値ｈａｓｈをスイッチ１４４６の接点Ｐｆを介して暗号化処理部１４０６へ与える。暗号化処理部１４０６は、ハッシュ値ｈａｓｈをセッションキーＫｓ２ａによって暗号化し、暗号化データ｛ｈａｓｈ｝Ｋｓ２ａを生成する（ステップＳ６０８）。

【０２１２】図２１を参照して、メモリカード１１０のコントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａを生成し、バスＢＳ４、インタフェース１４２４、および端子１４２６を介してライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａを出力する（ステップＳ６１０）。コントローラ５１０は、端子５８０、ＵＳＢインタフェース５５０を介してメモリカード１１０からライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａを受信する（ステップＳ６１２）。そして、コントローラ５１０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａとエントリ番号を指定したライセンス返却確認要求とをバスＢＳ２を介して貸出元であるライセンス管理デバイス５２０へ入力する（ステップＳ６１４）。

【０２１３】ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ２を介してライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ａとエントリ番号とライセンス返却確認要求とを受理する（ステップＳ６１６）。そして、コントローラ５２２０は、受理したライセンスＩＤが貸出時のライセンスＩＤに一致するか否かを判定し（ステップＳ６１８）、不一致であれば返却動作は終了する（ステップＳ６３８）。そして、ステップＳ６１８において、２つのライセンスＩＤが一致すると判定されたとき、コントローラ５２２０は、メモリカード１１０におけるライセンスの検索結果ｓｔａｔｅを確認する（ステップＳ６２０）。すなわち、コントローラ５２２０は、返却しようとするライセンスがメモリカード１１０のライセンス領域１４１５Ａから本当に消去されているか否かを確認し、ライセンス領域１４１５Ａにライセンスが存在するとき、返却動作を終了する（ステップＳ６３８）。そして、コントローラ５２２０は、返却しようとするライセンスがメモリカード１１０のライセンス領域１４１５Ａから消去されていることを確認したとき、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅのハッシュ値ｈａｓｈを求める（ステップＳ６２２）。つまり、ライセンス管理デバイス５２０のコントローラ５２２０は、自らライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ａ／／ｓｔａｔｅに対する署名を行ない、ハッシュ値ｈａｓｈを求める。

【０２１４】その後、コントローラ５２２０は、ステップＳ５５４において受理した｛ｈａｓｈ｝Ｋｓ２ａを復号処理部５２１２に与える。復号処理部５２１２は、｛ｈａｓｈ｝Ｋｓ２ａをセッションキーＫｓ２ａによって復号し、コントローラ５２２０は、メモリカード１１０におけるハッシュ値ｈａｓｈを受理する（ステップＳ６２４）。そして、コントローラ５２２０は、自ら求めたハッシュ値ｈａｓｈがメモリカード１１０におけるハッシュ値ｈａｓｈに一致するか否かを判定し（ステップＳ６２６）、不一致であるとき、メモリカード１１０における署名が書換えられていることになるので返却動作は終了する（ステップＳ６３８）。２つのハッシュ値が一致したとき、コントローラ５２２０は、ステップＳ６１６において受理した暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを復号処理部５２１２に与える。復号処理部５２１２は、暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａをセッションキーＫｓ２ａによって復号してセッションキーＫｓ２ｂを受理する（ステップＳ６２８）。

【０２１５】そして、コントローラ５２２０は、セッションキーＫｓ２ｂの確認を行ない（ステップＳ６３０）、ライセンスの貸出時にメモリカード１１０から受信したセッションキーＫｓ２ｂと不一致であれば返却動作は終了する（ステップＳ６３８）。ステップＳ６３０において２つのセッションキーＫｓ２ｂが一致したとき、コントローラ１４２０は、エントリ番号によって指定されたエントリ内の貸出フラグを「可」に変更する（ステップＳ６３２）。そして、コントローラ４０は、返却したライセンスの情報を削除し、貸出先のメモリカード１１０のデータ領域１４１５Ｂに記録されているライセンス管理情報および再生リストファイルを更新し、返却動作が終了する（ステップＳ６３８）。

【０２１６】このように、暗号化コンテンツデータおよびライセンスを貸出した相手先から暗号化コンテンツデータおよびライセンスを返却して貰うことによって、ライセンス管理デバイス５２０にライセンスを残したまま、携帯電話機１００および再生端末１０２において暗号化コンテンツデータを再生して楽しむことができる。

【０２１７】また、メモリカードへ貸出されたライセンスは、アクセス制御情報ＡＣｍによってメモリカードから他の記録機器（メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール）に対して、チェックアウトしたライセンスが出力できないよう指定されているため、貸出したライセンスが流出することはない。貸出したライセンス管理モジュールに対してチェックイン（返却）することで、貸出したライセンスの権利が、貸出したライセンス管理デバイスに戻るようになっている。したがって、著作者の意に反して複製ができること

を許すものではなく、セキュリティレベルが低下する処理ではなく、著作権も保護されている。

【０２１８】図２２を参照して、パーソナルコンピュータ５０のライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ５０のＨＤＤ５３０は、コンテンツリストファイル１５０と、コンテンツファイル１５３１～１５３５と、ライセンス管理ファイル１５２１～１５２５とを含む。

【０２１９】コンテンツリストファイル１５０は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルとを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Ｄｃ－ｉｎｆから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、ライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

【０２２０】コンテンツファイル１５３１～１５３５は、ライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを記録するファイルであり、コンテンツごとに設けられる。

【０２２１】また、ライセンス管理ファイル１５２１～１５２５は、それぞれ、コンテンツファイル１５３１～１５３５に対応して記録されており、ライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信されたライセンスを管理するためのファイルである。これまでの説明でも明らかなように、ライセンスは通常参照することができないが、ライセンス鍵Ｋｃを除く他の情報は、ユーザが書き換えることさえできなければ著作権保護の点では問題ない。しかし、運用においてライセンス鍵Ｋｃと分離して管理することはセキュリティの低下につながるため好ましくない。そこで、ライセンス配信を受ける場合に平文にて参照できるトランザクションＩＤ、コンテンツＩＤや、ライセンス購入条件ＡＣから容易に判断できるアクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐにて制限されている事項の写しおよびチェックアウトの記録を平文にて記録する。さらに、ライセンス管理デバイス５２０にライセンスが記録された場合にはエントリ番号を記録する。

【０２２２】ライセンス管理ファイル１５２１，１５２２，１５２４，１５２５は、それぞれ、エントリ番号０，２，１，３を含む。これは、ライセンス管理デバイス５２０によって受信され、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ａにおいて管理されるライセンス（ライセンスＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｍ）の管理領域を指定する番号である。

【０２２３】また、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ移動させるとき、コンテンツファイル１５３１～１５３５を検索してコンテンツファイル１５３１を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル１５３１に対応するライセンス管理ファイル１５２１に含まれるエントリ番号は「０」であるので、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ａのエントリ番号０によって指定された領域に記録されている。そうすると、ＨＤＤ５３０に記録されたコンテンツリストファイル１５０のライセンス管理ファイル１５２１からエントリ番号０を読出し、その読出したエントリ番号０をライセンス管理デバイス５２０に入力することによって、メモリ５２１５のライセンス領域５２１５Ａからライセンスを容易に取出し、メモリカード１１０へ移動できる。そして、ライセンスを移動した後は、メモリ５２１５のライセンス領域５２１５Ａにおいて指定されたエントリ番号内の有効フラグが「無効」にされるので（図１５のステップＳ３４６参照）、それに対応してライセンス管理ファイル１５２３のように「ライセンス無」が記録される。

【０２２４】ライセンス管理ファイル１５２３は、「ライセンス無」を含む。これは、ライセンス管理デバイス５２０によって受信されたライセンスが、移動された結果である。対応するコンテンツファイル１５３３はＨＤＤ５３０に記録されたままになっている。メモリカードからライセンスを再びライセンス管理モジュール５２０へ移動、あるいは、配信サーバ１０から再び配信を受ける場合には、ライセンスについてのみ配信を受けることが可能である。

【０２２５】貸出および返却においても、同様にエントリ番号を指定して処理することができる。また、貸出においては、ライセンス管理ファイルは、貸出の有無および貸出先を特定するための情報、たとえば、メモリカードに割当てられたメディアＩＤ等および貸出時のライセンスＩＤを記録する。これらの情報は、返却時に消去される。

【０２２６】このように、本発明においては、ライセンス管理デバイス５２０に記録されているライセンスをライセンス管理デバイス５２０に残したまま、セキュリティレベルを低下させることなく、著作権を保護しながら暗号化コンテンツデータの再生を携帯電話機１００や再生端末１０２によって自由に行なうことができる。

【０２２７】図２３は、メモリカード１１０のメモリ１

４１５におけるライセンス領域１４１５Ａとデータ領域１４１５Ｂとを示したものである。データ領域１４１５Ｂには、再生リストファイル１６０とコンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとが記録されている。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを１つのファイルとして記録する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記録されている。パーソナルコンピュータ５０におけるＨＤＤ５３０に記録されていた各データがメモリカード１１０のメモリ１４１５のデータ領域１４１５Ｂに記録されているのみで、他の点は、図２２と同じである。

【０２２８】また、ライセンス管理ファイル１６２２は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル１６１２は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、再生端末が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【０２２９】また、コンテンツファイル１６１３は、点線で示されているが、これは、たとえば、再生端末が配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけをパーソナルコンピュータ５０へ送信した場合に相当し、ライセンスはメモリ１４１５に存在するが暗号化コンテンツデータが存在しないことを意味する。

【０２３０】なお、ライセンス管理領域１４１５Ａは、ライセンス管理デバイスのライセンス管理領域５２１５Ａと同じ構成になっている。したがって、メモリカード１１０から他のメモリカードへの貸出し、さらにはライセンス管理デバイス５２０への貸出しも可能である。

【０２３１】［再生］上述したように、携帯電話機１００または再生端末１０２に装着されたメモリカード１１０は、配信サーバ１０から、直接、暗号化コンテンツデータおよびライセンスを受信できる。また、メモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０からハード的に取得した暗号化コンテンツデータおよびライセンスを、「移動」という概念によってパーソナルコンピュータ５０から受信できる。さらに、メモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０または音楽ＣＤからソフト的に取得した暗号化コンテンツデータおよびライセンスを、「貸出」という概念によってパーソナルコンピュータ５０から受信できる。

【０２３２】このように、メモリカード１１０は、各種の方法によって暗号化コンテンツデータおよびライセンスを受信する。そこで、次に、これらの各種の方法によってメモリカードが受信した暗号化コンテンツデータの再生について説明する。

【０２３３】図２４は、メモリカード１１０が受信したコンテンツデータの再生端末１０２における再生動作を説明するためのフローチャートである。なお、図２４における処理以前に、再生端末１０２のユーザは、メモリカード１００のデータ領域１４１５Ｂに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【０２３４】図２４を参照して、再生動作の開始とともに、再生端末１００のユーザから操作パネル１１０８を介して再生リクエストが再生端末１００にインプットされる（ステップＳ７００）。そうすると、コントローラ１１０６は、バスＢＳ３を介して認証データの出力要求をコンテンツ再生回路１５５０に行ない（ステップＳ７０２）、コンテンツ再生回路１５５０は認証データの出力要求を受信する（ステップＳ７０４）。そして、認証データ保持部１５００は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力し（ステップＳ７０６）、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを入力する（ステップＳ７０８）。

【０２３５】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理し、復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ７１０）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ７１２）。復号できなかった場合、ステップＳ７４８へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、セッションキー発生部１４１８を制御し、セッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ７１４）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ７１６）。再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、コントローラ１１０６は、｛Ｋｓ２｝Ｋｐ１をバスＢＳ３を介してコンテンツ再生回路１５５０の復号処理部１５０４へ与え（ステップＳ７１８）、復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開

暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ７２０）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ７２２）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し（ステップＳ７２４）、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ７２６）。

【０２３６】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して｛Ｋｓ３｝Ｋｓ２を入力する。復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、再生端末１００で発生されたセッションキーＫｓ３を受理する（ステップＳ７２８）。

【０２３７】再生端末のコントローラ１１０６は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し（ステップＳ７３０）、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号とライセンスの出力要求を出力する（ステップＳ７３２）。

【０２３８】メモリカード１１０のコントローラ１４２０は、エントリ番号とライセンスの出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する（ステップＳ７３４）。

【０２３９】そして、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ７３６）。

【０２４０】ステップＳ７３６においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ＡＣｍの再生回数を変更した（ステップＳ７３８）後に次のステップ（ステップＳ７４０）に進む。一方、アクセス制限情報ＡＣｍの再生回数によって再生が制限されていない場合においては、ステップＳ７３８はスキップされ、アクセス制限情報ＡＣｍの再生回数は変更されることなく処理が次のステップ（ステップＳ７４０）に進行される。

【０２４１】ステップＳ７３６において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ａに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生制御情報ＡＣｐがバスＢＳ４上に出力される（ステップＳ７４０）。

【０２４２】得られたライセンス鍵Ｋｃと再生制御情報ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生制御情報ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ４に出力する（ステップＳ７４０）。

【０２４３】バスＢＳ４に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して再生端末１０２に送出される。

【０２４４】再生端末１０２においては、メモリカードインタフェース１２００を介してバスＢＳ３に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受理する（ステップＳ７４２，Ｓ７４４）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生制御情報ＡＣｐをバスＢＳ３に出力する。

【０２４５】コントローラ１１０６は、バスＢＳ３を介して、再生制御情報ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ７４６）。

【０２４６】ステップＳ７４６においては、再生制御情報ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０２４７】ステップＳ７４６において再生可能と判断された場合、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ４、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する。

【０２４８】再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをコンテンツ再生回路１５５０へ与える。

【０２４９】そして、コンテンツ再生回路１５５０の復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたライセンス鍵Ｋｃによって復号してコンテンツデータＤｃを取得する。

【０２５０】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８

は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーン１３０へ出力されて再生される。これによって再生動作が終了する（ステップＳ７４８）。

【０２５１】本発明の実施の形態によれば、貸出元のメモリカードは、貸出したライセンスを貸出先ＩＤおよび貸出時ライセンスＩＤによって管理し、ライセンスの貸出を貸出フラグによって管理し、ライセンスの貸出時に貸出用ライセンスを自己が保持したライセンスから生成し、元のライセンスが貸出中であることを示すフラグを貸出フラグに設定するので、貸出したライセンスのバックアップを提供することができる。

【０２５２】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０２５３】

【発明の効果】本発明によれば、貸出元のメモリカードは、貸出したライセンスを貸出先ＩＤおよび貸出時ライセンスＩＤによって管理し、ライセンスの貸出を貸出フラグによって管理し、ライセンスの貸出時に貸出用ライセンスを自己が保持したライセンスから生成し、元のライセンスが貸出中であることを示すフラグを貸出フラグに設定するので、貸出したライセンスのバックアップを提供することができる。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　他のデータ配信システムを概念的に説明する概略図である。

【図３】　図１および図２に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１および図２に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　図１および図２に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図６】　図１および図２に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図７】　図２に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

【図８】　図１および図２に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図９】　図６に示すライセンス管理デバイスの構成を示す概略ブロック図である。

【図１０】　図１および図２に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図１１】　図１および図２に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１２】　リッピングを実行するソフトウエアの機能を説明するための機能ブロック図である。

【図１３】　図１および図２に示すデータ配信システムにおけるリッピングの動作を説明するためのフローチャートである。

【図１４】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第１のフローチャートである。

【図１５】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第２のフローチャートである。

【図１６】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの貸出動作を説明するための第１のフローチャートである。

【図１７】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの貸出動作を説明するための第２のフローチャートである。

【図１８】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第１のフローチャートである。

【図１９】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第２のフローチャートである。

【図２０】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第３のフローチャートである。

【図２１】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第４のフローチャートである。

【図２２】　パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

【図２３】　メモリカードにおける再生リストファイルの構成を示す図である。

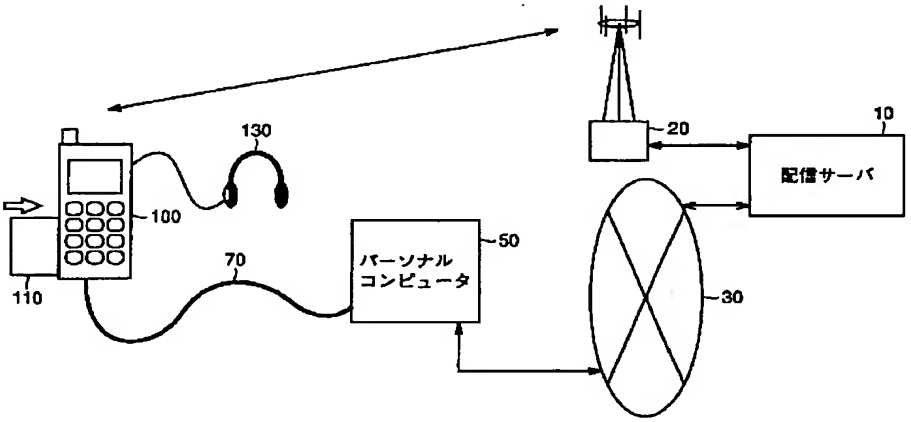
【図２４】　再生端末における再生動作を説明するためのフローチャートである。

【符号の説明】

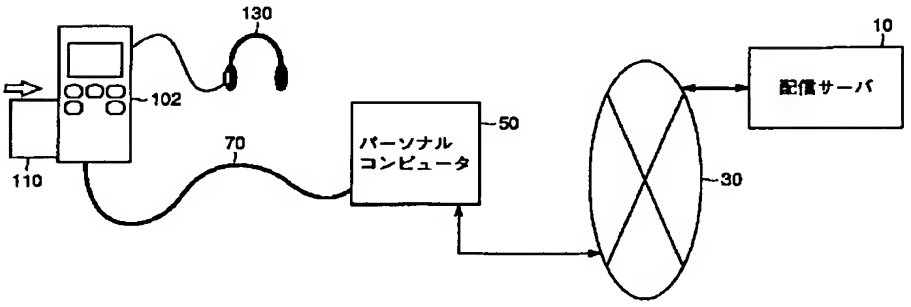
１０　配信サーバ、２０　配信キャリア、３０　インターネット網、５０　パーソナルコンピュータ、６０　音楽ＣＤ、７０　ＵＳＢケーブル、１００　携帯電話機、１０２　再生端末、１１０　メモリカード、１３０　ヘッドホーン、１５０　コンテンツリストファイル、１６

０　再生リストファイル、３０２　課金データベース、３０４　情報データベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６，５２０４，５２０８，５２１２，５２２２　復号処理部、３１３　認証鍵保持部、３１５配信制御部、３１６，　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６，５２０６，５２１０，５２１７，５４０５　暗号処理部、３５０　通信装置、５１０，１１０６，１４２０，５２２０コントローラ、５２０　ライセンス管理デバイス、５３０　ハードディスク、５５０，１１１２　ＵＳＢインタフェース、５５５　モデム、５６０　キーボード、５７０　ディスプレイ、５８０，１１１４，１４２６，１５３０，５２２６端子、１１０８　操作パネル、１１１０　表示パネル、１２００　メモリカードインタフェース、１４００，１５００，５２００　認証データ保持部、１４０２，５２０２　Ｋｍｃ保持部、１４１４，５２１４　ＫＰａ保持部、１４１５，５２１５　メモリ、１４１５Ａ　ライセンス領域、１４１５Ｂ　データ領域、１４１６，５２１６　ＫＰｍｃ保持部、１４１８，５２１８　セッションキー発生部、１４２１，５２２１　Ｋｍ保持部、１４２４，５２２４　インタフェース、１４４２，１４４６，５２４２，５２４６　切換スイッチ、１５０２　Ｋｐ１保持部、１５１８　音楽再生部、１５１９　ＤＡ変換器、１５２１～１５２５，１６２１～１６２ｎ　ライセンス管理ファイル、１５３１～１５３５，１６１１～１６１ｎ　コンテンツファイル、１５５０　コンテンツ再生回路、５４００　ウォータマーク検出手段、５４０１　ウォータマーク判定手段、５４０２　リマーク手段、５４０３　ライセンス発生手段、５４０４　音楽エンコーダ。

【図１】




【図２】



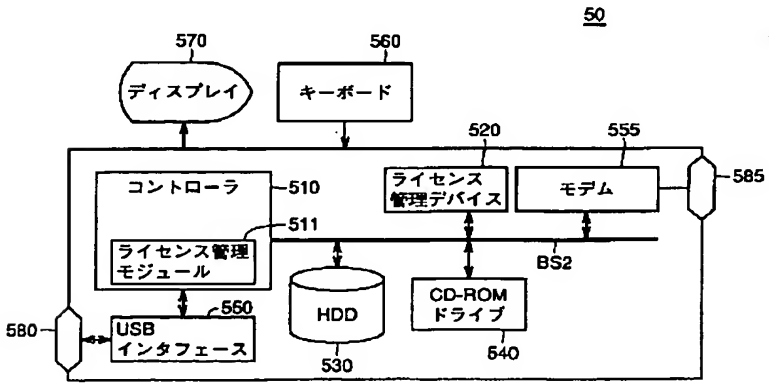
【図３】

| 記号 | 種類 | 属性 | 特性 |
|---|---|---|---|
| Dc | コンテンツデータ | コンテンツ固有 | 例：音楽データ、朗読データ、教材データ、画像データ<br>Kcにて復号可能な暗号化コンテンツデータ<br>{Dc}Kcとして配信され、メモリカードに保持される |
| Dc-Inf | 付加情報 | コンテンツ固有 | Dcに付随する平文データ。 |
| Kc | ライセンス | コンテンツ固有 | ライセンス<br>暗号化コンテンツデータを復号する復号鍵 |
| ACm/ACp | ライセンス | ライセンス固有 | 制限情報<br>再生やライセンスの取り扱いに対する制限事項 |
| コンテンツID | ライセンス | コンテンツ固有 | コンテンツを特定するための管理コード |
| ライセンスID | ライセンス | ライセンス固有 | ライセンスを特定するための管理コード |
| ライセンス | ライセンス | ライセンス固有 | Kc＋ACm＋ACp＋コンテンツID＋ライセンスIDの総称 |
| 有効フラグ | フラグ | ライセンス固有 | ライセンスをメモリカードから外部へ出すことが可能か否かを表す。 |
| 貸出フラグ | フラグ | ライセンス固有 | ライセンスの貸出の可否を表す。 |
| 貸出先ID | 特定情報 | メモリカード固有 | ライセンスを貸出した貸出先を特定するための情報 |
| 貸出時ライセンスID | 識別情報 | ライセンス固有 | 貸出したライセンスを識別するための情報 |

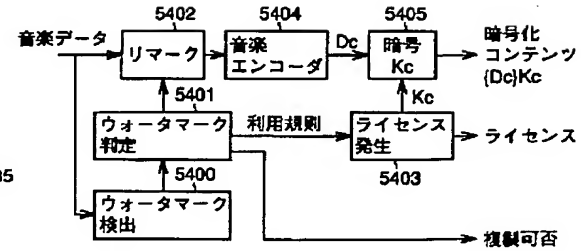
【図４】

| | 記号 | 種類 | 属性 | 特性 |
|---|---|---|---|---|
| 配信サーバ | KPa | 公開認証鍵 | システム共通 | 認証局にて認証データを復号する鍵 |
| | Ks1 | 共通鍵 | セッション固有 | メモリカード、ライセンス管理デバイスへのライセンス配信ごとに発生 |
| メモリカード<br>ライセンス管理デバイス | KPa | 公開認証鍵 | システム共通 | 認証局にて認証データを復号する鍵<br>配信サーバのKPaと同一 |
| | KPmw | 公開暗号鍵 | クラス固有 | 証明書Cmwとともに認証局にて暗号化された認証データとして保持<br>wはクラスを識別するための識別子 |
| | Kmw | 秘密復号鍵 | クラス固有 | 公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵 |
| | KPmcx | 公開暗号鍵 | 個別 | メモリカードごとに異なる。<br>xはモジュールを識別するための識別子 |
| | Kmcx | 秘密復号鍵 | 個別 | 公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵 |
| | Ks2 | 共通鍵 | セッション固有 | ライセンスの授受ごとに発生 |
| | Cmw | 証明書 | クラス証明書 | メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。認証機能を有する。<br>{KPmw//Cmw}KPaの形式で出荷時に記録。<br>＊メモリカードおよびライセンス管理デバイスのクラスwごとに異なる。 |
| コンテンツ再生回路 | KPpy | 公開暗号鍵 | クラス固有 | 証明書Cmwとともに認証局にて暗号化された認証データとして保持<br>yはクラスを識別するための識別子 |
| | Kpy | 秘密復号鍵 | クラス固有 | 公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵 |
| | Ks3 | 共通鍵 | セッション固有 | 配信サーバまたは音楽再生モジュール間の再生セッションごとに発生 |
| | Cpy | 証明書 | クラス証明書 | コンテンツ再生回路のクラス証明書。認証機能を有する。<br>{KPpy//Cpy}KPaの形式で出荷時に記録。<br>＊コンテンツ再生回路のクラスyごとに異なる。 |

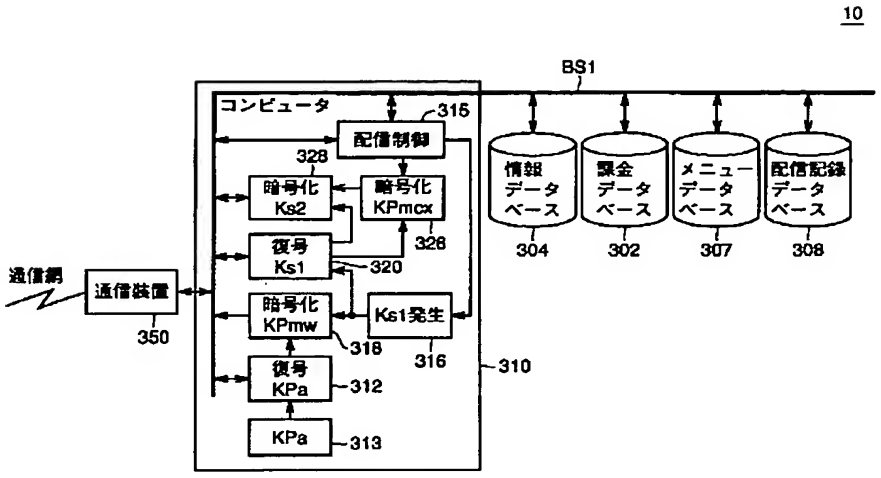
【図６】



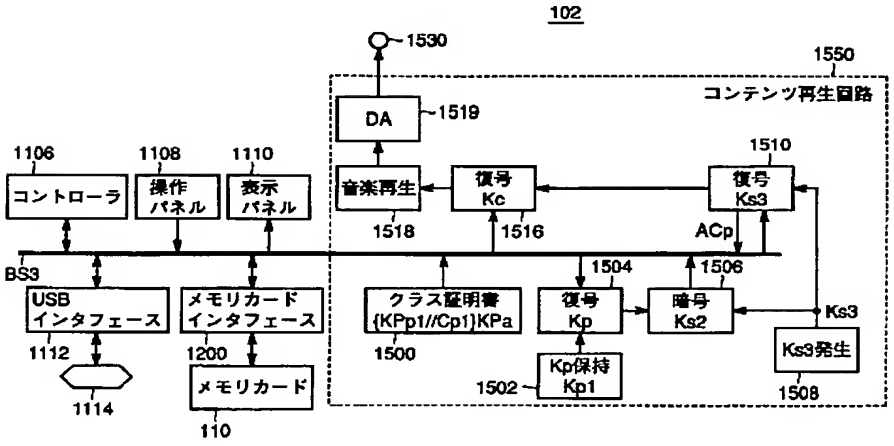

【図１２】



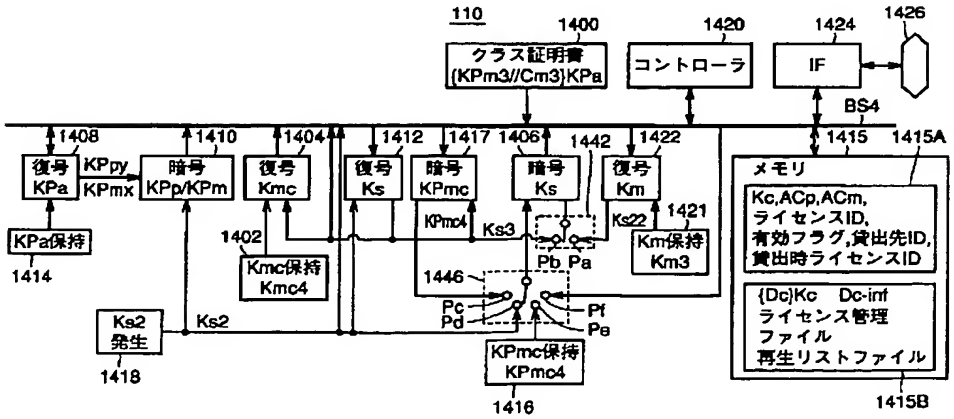
【図５】


10
BS1
コンピュータ
315
配信制御
328
暗号化 Ks2
暗号化 KPmcx
326
復号 Ks1
320
暗号化 KPmw
318
Ks1発生
316
復号 KPa
312
KPa
313
310
通信網
通信装置
350
情報データベース
304
課金データベース
302
メニューデータベース
307
配信記録データベース
308

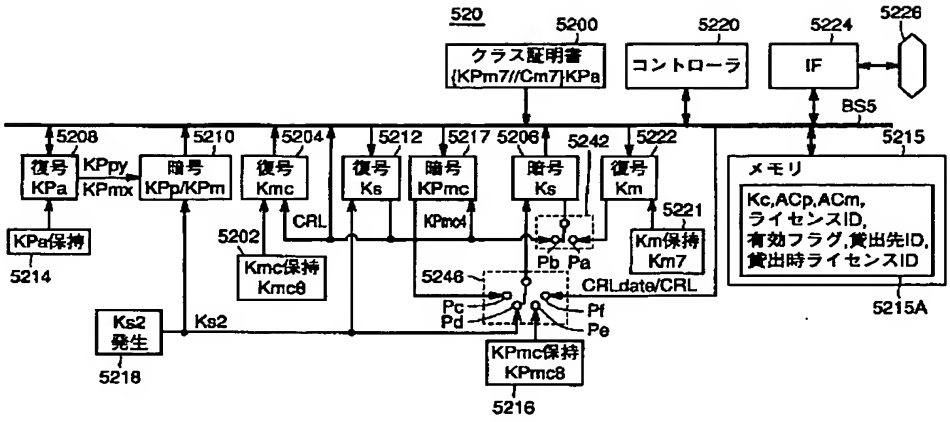
【図７】


102
1530
1550
コンテンツ再生回路
DA
1519
1106
1108
1110
コントローラ
操作パネル
表示パネル
音楽再生
1518
復号 Kc
1516
1510
復号 Ks3
ACp
BS3
1504
1506
USB インタフェース
1112
1114
メモリカード インタフェース
1200
メモリカード
110
クラス証明書 {KPp1//Cp1}KPa
1500
復号 Kp
暗号 Ks2
Ks3
Kp保持 Kp1
1502
Ks3発生
1508

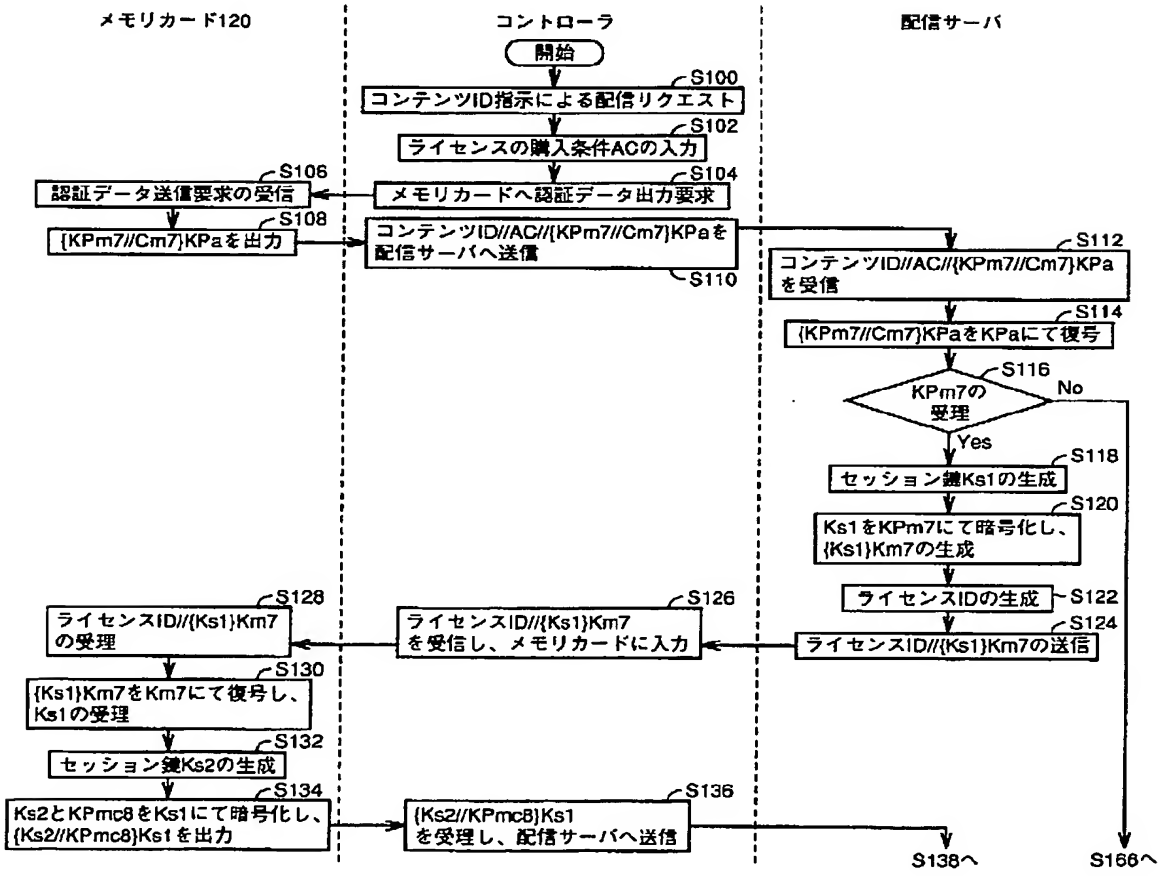
【図８】


110
1400
クラス証明書 {KPm3//Cm3}KPa
1420
コントローラ
1424
IF
1426
BS4
1408
1410
1404
1412
1417
1406
1442
1422
1415
1415A
復号 KPa
KPpy KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
メモリ
Kc,ACp,ACm, ライセンスID, 有効フラグ,貸出先ID, 貸出時ライセンスID
KPa保持
1414
1402
Kmc保持 Kmc4
KPmc4
Ks3
Ks22
1421
Km保持 Km3
Pb, Pa
1446
Pc
Pd
Pf
Pe
{Dc}Kc Dc-inf ライセンス管理ファイル 再生リストファイル
Ks2 発生
1418
Ks2
KPmc保持 KPmc4
1416
1415B

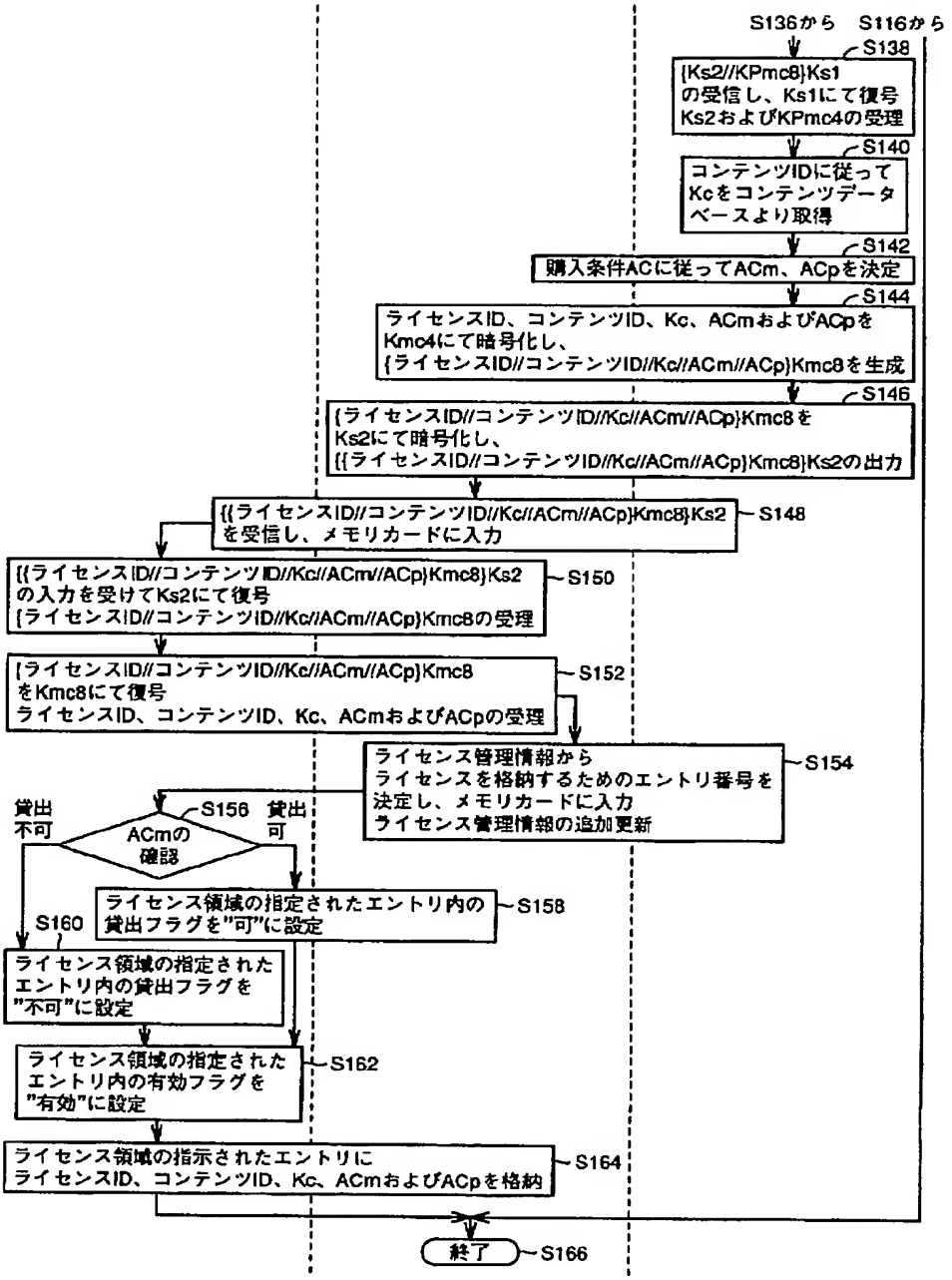
【図９】


520
5200
クラス証明書
{KPm7//Cm7}KPa
5220
コントローラ
5224
IF
5226
BS5
5208
5210
5204
5212
5217
5206
5242
5222
5215
復号
KPa
KPpy
KPmx
暗号
KPp/KPm
復号
Kmc
復号
Ks
暗号
KPmc
暗号
Ks
復号
Km
メモリ
Kc,ACp,ACm,
ライセンスID,
有効フラグ,貸出先ID,
貸出時ライセンスID
5215A
KPa保持
5214
5202
CRL
Kmc保持
Kmc8
KPmc4
5221
Km保持
Km7
Pb Pa
5246
CRLdate/CRL
Pc
Pd
Pf
Pe
Ks2
発生
5218
Ks2
KPmc保持
KPmc8
5216

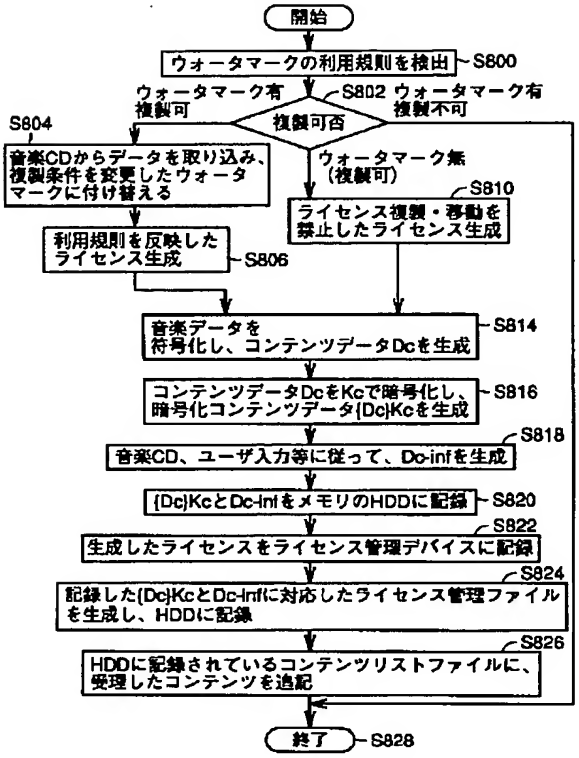
【図１０】


メモリカード120
コントローラ
配信サーバ
開始
S100
コンテンツID指示による配信リクエスト
S102
ライセンスの購入条件ACの入力
S104
メモリカードへ認証データ出力要求
S106
認証データ送信要求の受信
S108
{KPm7//Cm7}KPaを出力
コンテンツID//AC//{KPm7//Cm7}KPaを
配信サーバへ送信
S110
S112
コンテンツID//AC//{KPm7//Cm7}KPa
を受信
S114
{KPm7//Cm7}KPaをKPaにて復号
S116
KPm7の
受理
No
Yes
S118
セッション鍵Ks1の生成
S120
Ks1をKPm7にて暗号化し、
{Ks1}Km7の生成
ライセンスIDの生成
S122
S124
ライセンスID//{Ks1}Km7の送信
S126
ライセンスID//{Ks1}Km7
を受信し、メモリカードに入力
S128
ライセンスID//{Ks1}Km7
の受理
S130
{Ks1}Km7をKm7にて復号し、
Ks1の受理
S132
セッション鍵Ks2の生成
S134
Ks2とKPmc8をKs1にて暗号化し、
{Ks2//KPmc8}Ks1を出力
S136
{Ks2//KPmc8}Ks1
を受理し、配信サーバへ送信
S138へ
S166へ

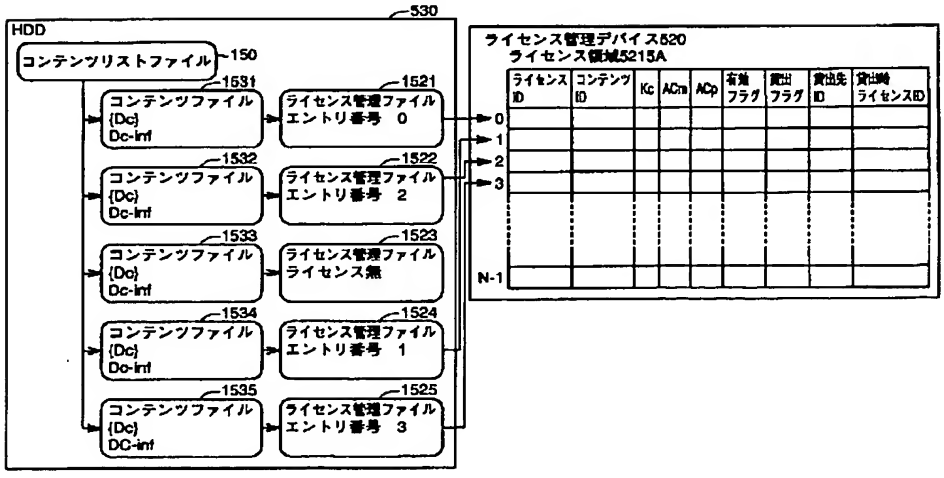
【図１１】


S136から S116から
S138
{Ks2//KPmc8}Ks1
の受信し、Ks1にて復号
Ks2およびKPmc4の受理
S140
コンテンツIDに従って
Kcをコンテンツデータ
ベースより取得
S142
購入条件ACに従ってACm、ACpを決定
S144
ライセンスID、コンテンツID、Kc、ACmおよびACpを
Kmc4にて暗号化し、
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8を生成
S146
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8を
Ks2にて暗号化し、
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の出力
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2
を受信し、メモリカードに入力
S148
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2
の入力を受けてKs2にて復号
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8の受理
S150
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc8
をKmc8にて復号
ライセンスID、コンテンツID、Kc、ACmおよびACpの受理
S152
ライセンス管理情報から
ライセンスを格納するためのエントリ番号を
決定し、メモリカードに入力
ライセンス管理情報の追加更新
S154
貸出
不可
S156
ACmの
確認
貸出
可
ライセンス領域の指定されたエントリ内の
貸出フラグを"可"に設定
S158
S160
ライセンス領域の指定された
エントリ内の貸出フラグを
"不可"に設定
ライセンス領域の指定された
エントリ内の有効フラグを
"有効"に設定
S162
ライセンス領域の指示されたエントリに
ライセンスID、コンテンツID、Kc、ACmおよびACpを格納
S164
終了
S166

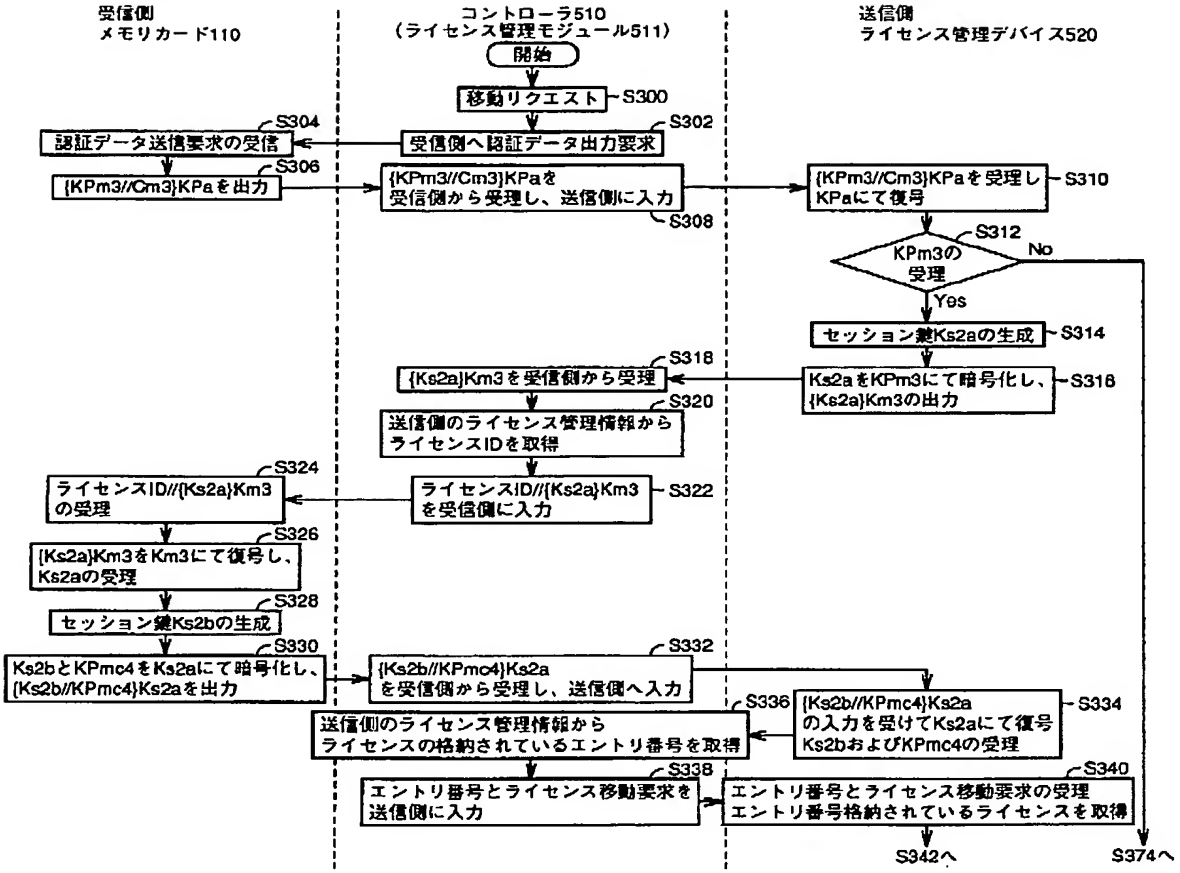
【図１３】


開始
ウォータマークの利用規則を検出
S800
ウォータマーク有
複製可
S802
複製可否
ウォータマーク有
複製不可
S804
音楽CDからデータを取り込み、複製条件を変更したウォータマークに付け替える
ウォータマーク無
（複製可）
S810
ライセンス複製・移動を禁止したライセンス生成
利用規則を反映したライセンス生成
S806
音楽データを符号化し、コンテンツデータDcを生成
S814
コンテンツデータDcをKcで暗号化し、暗号化コンテンツデータ{Dc}Kcを生成
S816
音楽CD、ユーザ入力等に従って、Dc-infを生成
S818
{Dc}KcとDc-infをメモリのHDDに記録
S820
生成したライセンスをライセンス管理デバイスに記録
S822
記録した{Dc}KcとDc-infに対応したライセンス管理ファイルを生成し、HDDに記録
S824
HDDに記録されているコンテンツリストファイルに、受理したコンテンツを追記
S826
終了
S828

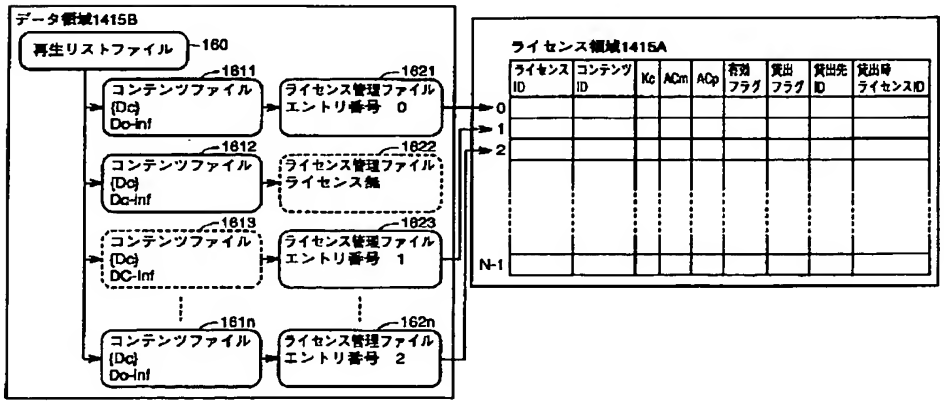
【図２２】


530
HDD
コンテンツリストファイル
150
1531
コンテンツファイル
{Dc}
Dc-inf
1521
ライセンス管理ファイル
エントリ番号 0
1532
コンテンツファイル
{Dc}
Dc-inf
1522
ライセンス管理ファイル
エントリ番号 2
1533
コンテンツファイル
{Dc}
Dc-inf
1523
ライセンス管理ファイル
ライセンス無
1534
コンテンツファイル
{Dc}
Dc-inf
1524
ライセンス管理ファイル
エントリ番号 1
1535
コンテンツファイル
{Dc}
DC-inf
1525
ライセンス管理ファイル
エントリ番号 3
ライセンス管理デバイス520
ライセンス領域5215A
ライセンスID
コンテンツID
Kc
ACm
ACp
有効フラグ
貸出フラグ
貸出先ID
貸出時ライセンスID
0
1
2
3
N-1

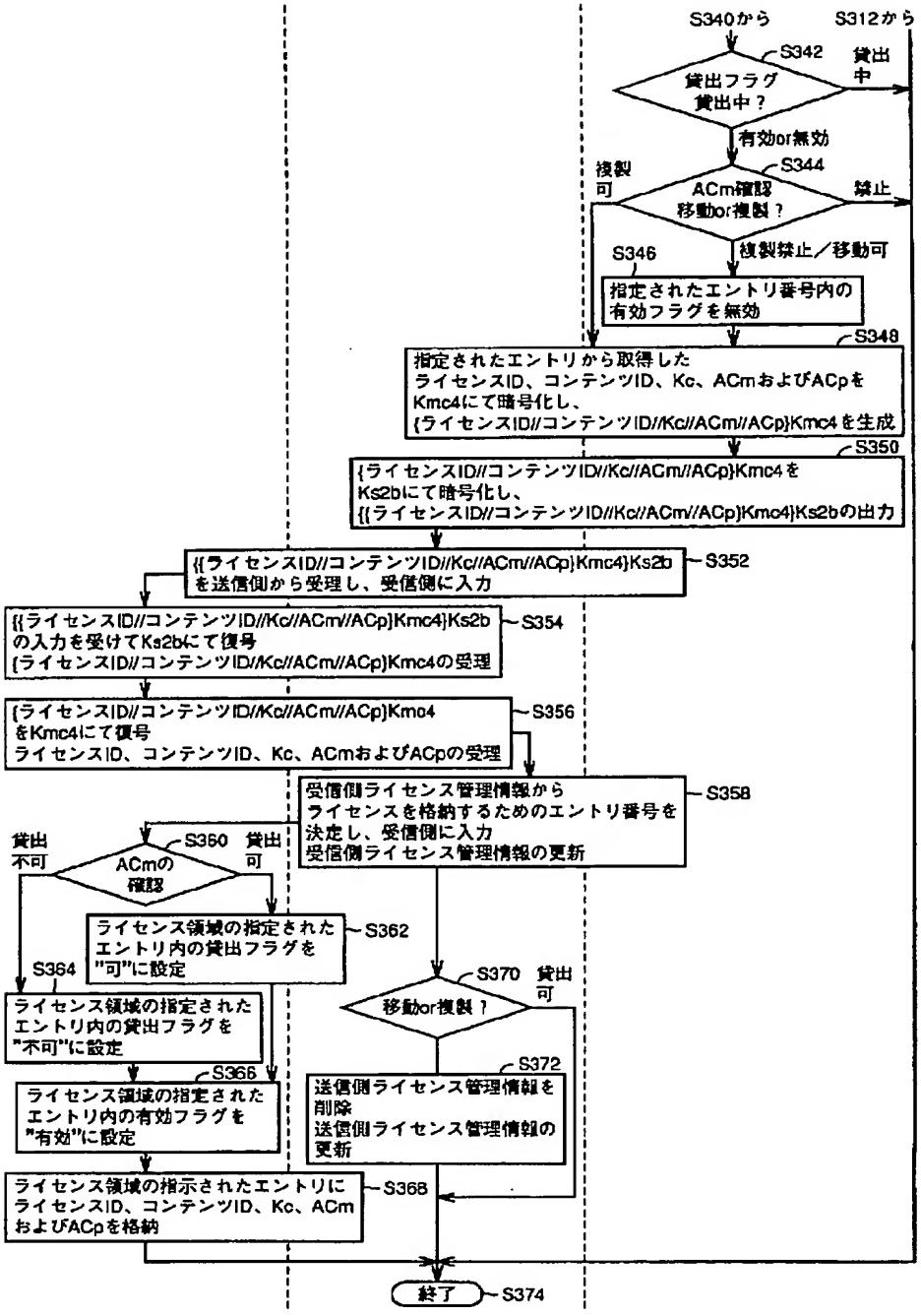
【図１４】


受信側
メモリカード110
コントローラ510
（ライセンス管理モジュール511）
送信側
ライセンス管理デバイス520
開始
移動リクエスト
S300
認証データ送信要求の受信
S304
受信側へ認証データ出力要求
S302
{KPm3//Cm3}KPaを出力
S306
{KPm3//Cm3}KPaを
受信側から受理し、送信側に入力
S308
{KPm3//Cm3}KPaを受理し
KPaにて復号
S310
KPm3の
受理
S312
No
Yes
セッション鍵Ks2aの生成
S314
{Ks2a}Km3を受信側から受理
S318
Ks2aをKPm3にて暗号化し、
{Ks2a}Km3の出力
S316
送信側のライセンス管理情報から
ライセンスIDを取得
S320
ライセンスID//{Ks2a}Km3
の受理
S324
ライセンスID//{Ks2a}Km3
を受信側に入力
S322
{Ks2a}Km3をKm3にて復号し、
Ks2aの受理
S326
セッション鍵Ks2bの生成
S328
Ks2bとKPmc4をKs2aにて暗号化し、
{Ks2b//KPmc4}Ks2aを出力
S330
{Ks2b//KPmc4}Ks2a
を受信側から受理し、送信側へ入力
S332
{Ks2b//KPmc4}Ks2a
の入力を受けてKs2aにて復号
Ks2bおよびKPmc4の受理
S334
送信側のライセンス管理情報から
ライセンスの格納されているエントリ番号を取得
S336
エントリ番号とライセンス移動要求を
送信側に入力
S338
エントリ番号とライセンス移動要求の受理
エントリ番号格納されているライセンスを取得
S340
S342へ
S374へ

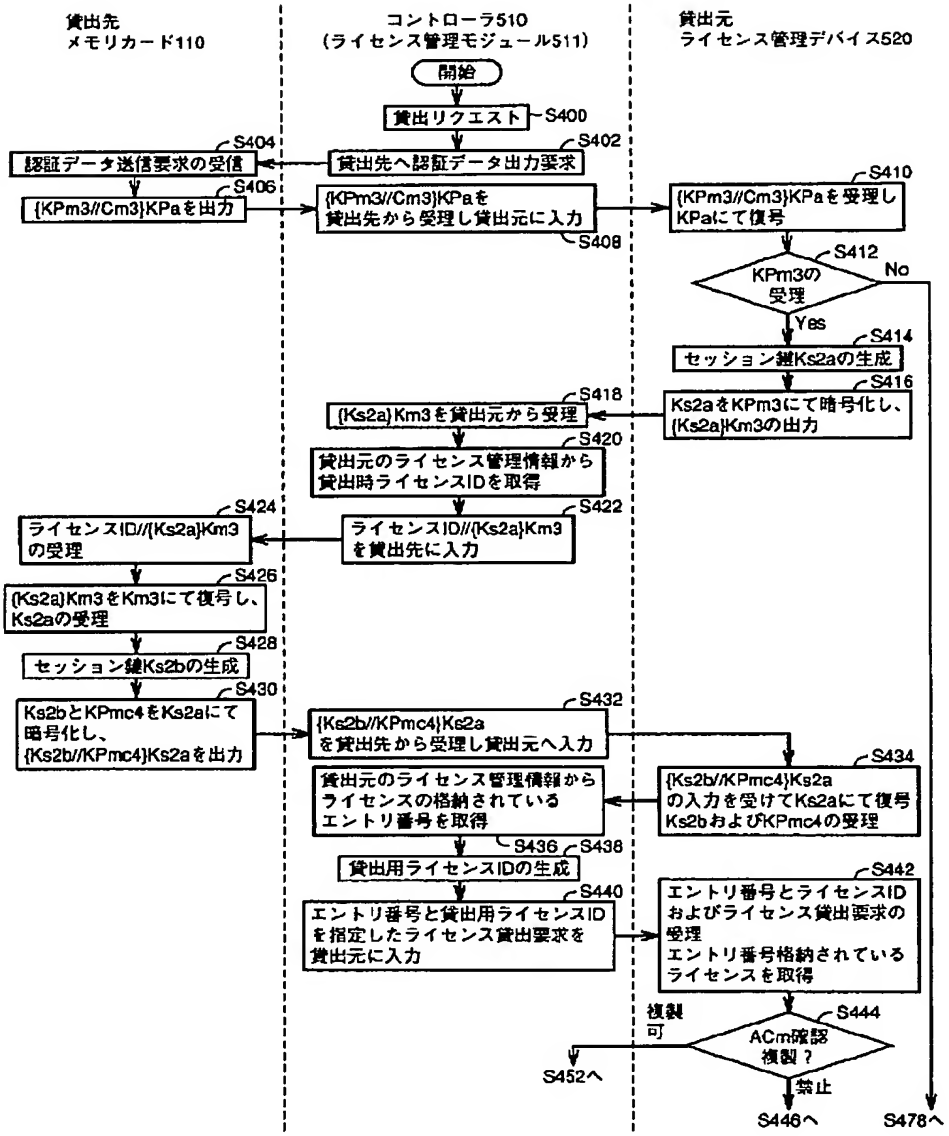
【図２３】


データ領域1415B
再生リストファイル
160
コンテンツファイル
{Dc}
Do-Inf
1611
ライセンス管理ファイル
エントリ番号 0
1621
コンテンツファイル
{Dc}
Do-Inf
1612
ライセンス管理ファイル
ライセンス無
1622
コンテンツファイル
{Dc}
DC-Inf
1613
ライセンス管理ファイル
エントリ番号 1
1623
コンテンツファイル
{Dc}
Do-Inf
161n
ライセンス管理ファイル
エントリ番号 2
162n
ライセンス領域1415A
ライセンスID
コンテンツID
Kc
ACm
ACp
有効フラグ
貸出フラグ
貸出先ID
貸出時ライセンスID
0
1
2
N-1

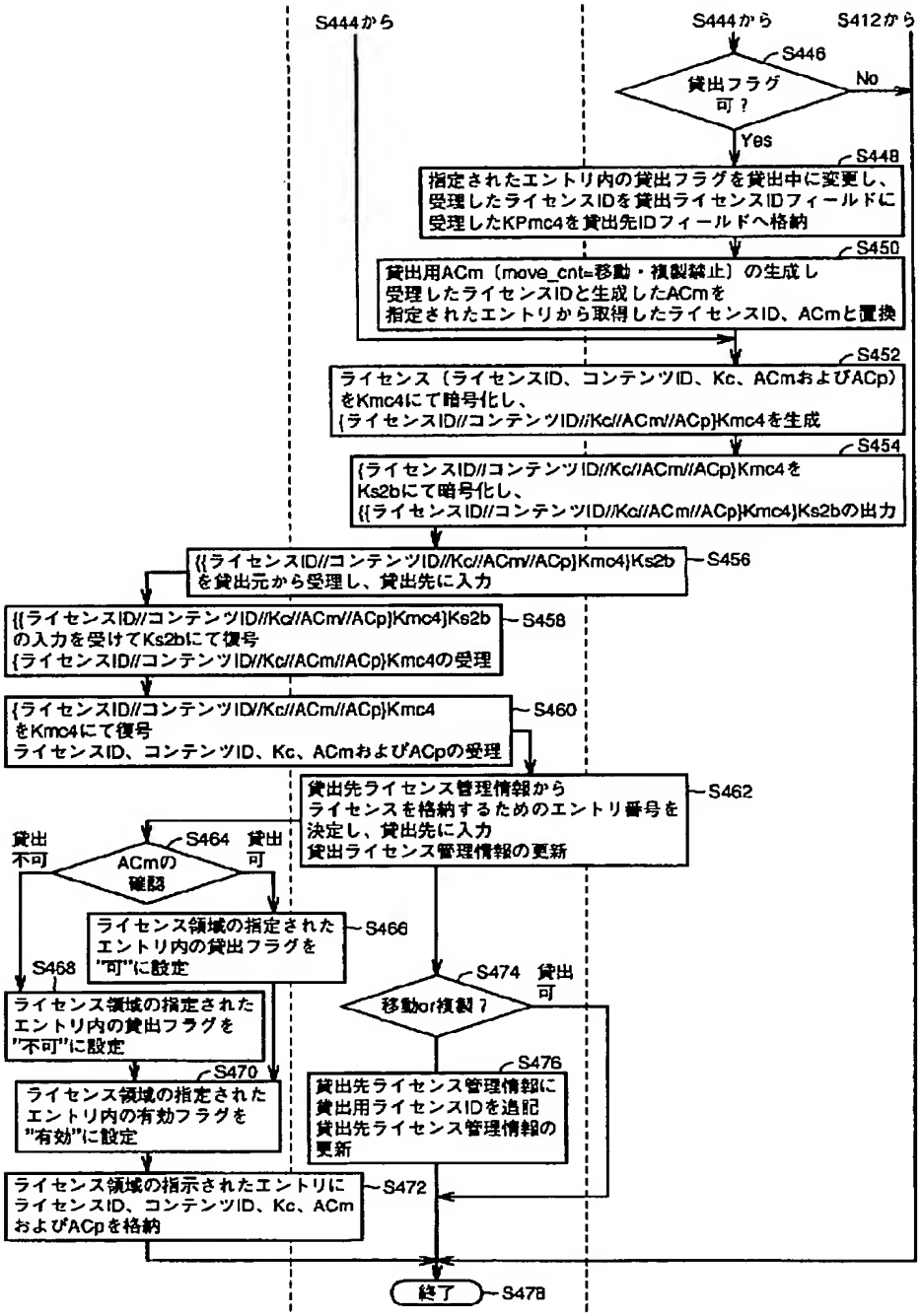
【図１５】


S340から
S312から
S342
貸出フラグ 貸出中？
貸出中
有効or無効
S344
複製可
ACm確認 移動or複製？
禁止
S346
複製禁止／移動可
指定されたエントリ番号内の有効フラグを無効
S348
指定されたエントリから取得したライセンスID、コンテンツID、Kc、ACmおよびACpをKmc4にて暗号化し、{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成
S350
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をKs2bにて暗号化し、{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの出力
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを送信側から受理し、受信側に入力
S352
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの入力を受けてKs2bにて復号{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4の受理
S354
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をKmc4にて復号ライセンスID、コンテンツID、Kc、ACmおよびACpの受理
S356
受信側ライセンス管理情報からライセンスを格納するためのエントリ番号を決定し、受信側に入力受信側ライセンス管理情報の更新
S358
貸出不可
S360
ACmの確認
貸出可
ライセンス領域の指定されたエントリ内の貸出フラグを"可"に設定
S362
S364
ライセンス領域の指定されたエントリ内の貸出フラグを"不可"に設定
S370
移動or複製？
貸出可
S372
送信側ライセンス管理情報を削除送信側ライセンス管理情報の更新
S366
ライセンス領域の指定されたエントリ内の有効フラグを"有効"に設定
ライセンス領域の指示されたエントリにライセンスID、コンテンツID、Kc、ACmおよびACpを格納
S368
終了
S374

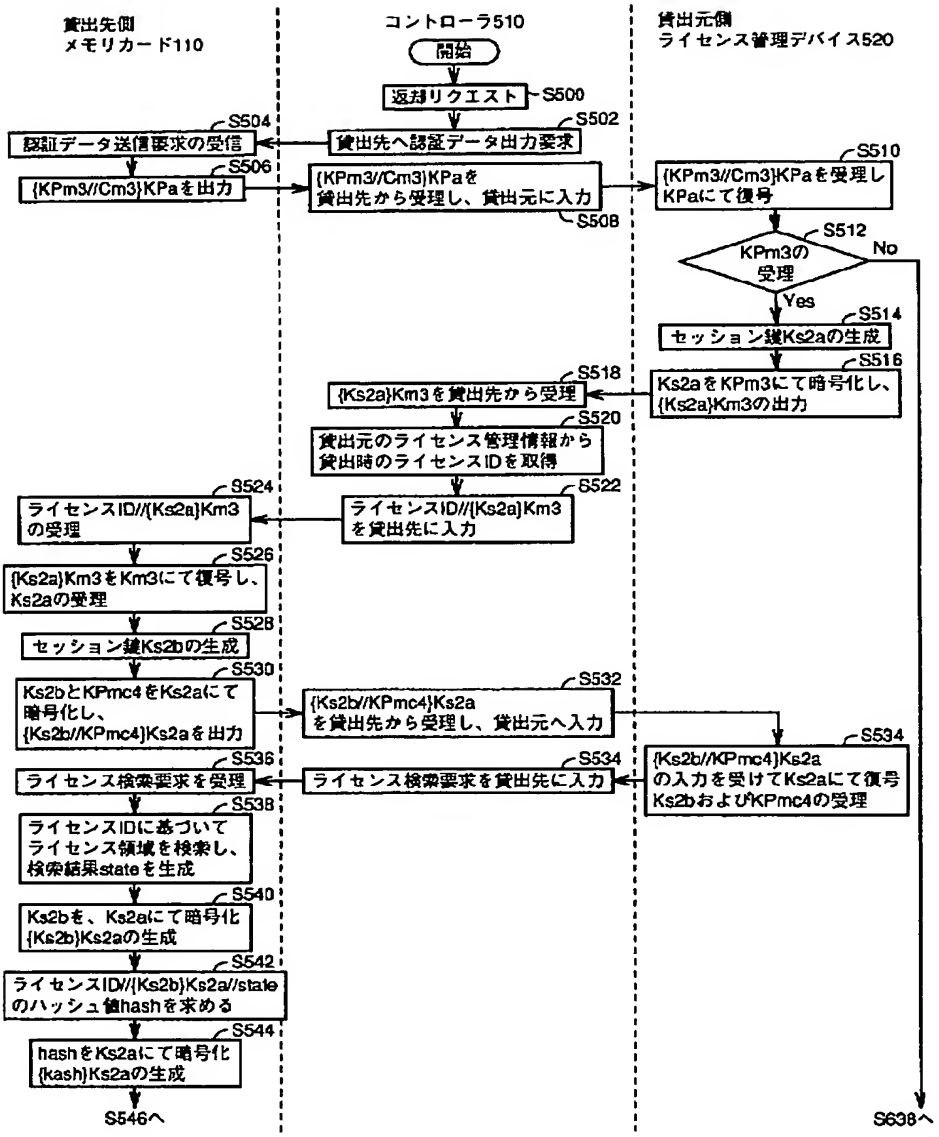
【図１６】


貸出先
メモリカード110
コントローラ510
（ライセンス管理モジュール511）
貸出元
ライセンス管理デバイス520
開始
貸出リクエスト
S400
S402
貸出先へ認証データ出力要求
S404
認証データ送信要求の受信
S406
{KPm3//Cm3}KPaを出力
{KPm3//Cm3}KPaを
貸出先から受理し貸出元に入力
S408
S410
{KPm3//Cm3}KPaを受理し
KPaにて復号
S412
KPm3の
受理
No
Yes
S414
セッション鍵Ks2aの生成
S416
Ks2aをKPm3にて暗号化し、
{Ks2a}Km3の出力
S418
{Ks2a}Km3を貸出元から受理
S420
貸出元のライセンス管理情報から
貸出時ライセンスIDを取得
S422
ライセンスID//{Ks2a}Km3
を貸出先に入力
S424
ライセンスID//{Ks2a}Km3
の受理
S426
{Ks2a}Km3をKm3にて復号し、
Ks2aの受理
S428
セッション鍵Ks2bの生成
S430
Ks2bとKPmc4をKs2aにて
暗号化し、
{Ks2b//KPmc4}Ks2aを出力
S432
{Ks2b//KPmc4}Ks2a
を貸出先から受理し貸出元へ入力
S434
{Ks2b//KPmc4}Ks2a
の入力を受けてKs2aにて復号
Ks2bおよびKPmc4の受理
貸出元のライセンス管理情報から
ライセンスの格納されている
エントリ番号を取得
S436
S438
貸出用ライセンスIDの生成
S440
エントリ番号と貸出用ライセンスID
を指定したライセンス貸出要求を
貸出元に入力
S442
エントリ番号とライセンスID
およびライセンス貸出要求の
受理
エントリ番号格納されている
ライセンスを取得
S444
複製
可
ACm確認
複製？
禁止
S452へ
S446へ
S478へ

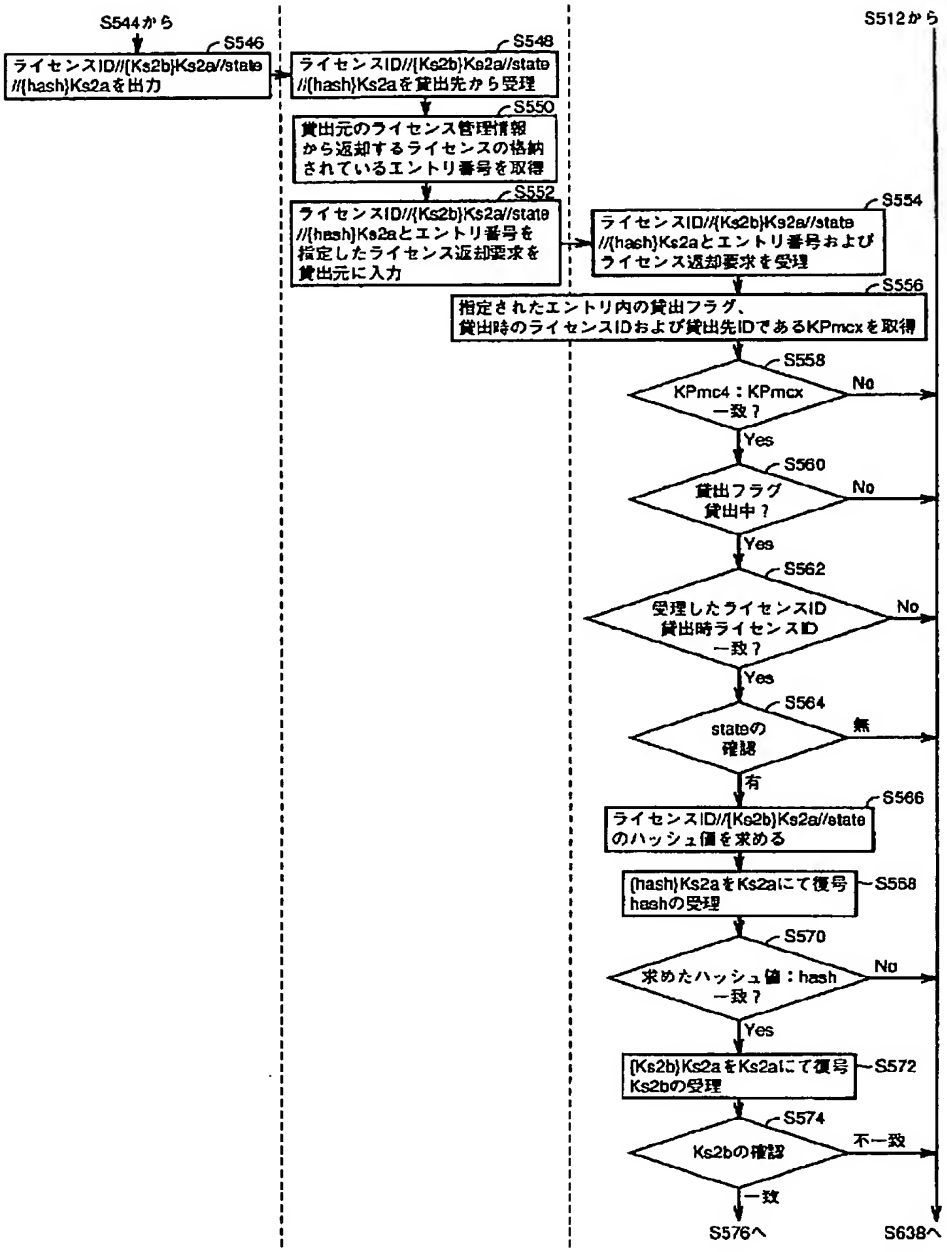
【図１７】


S444から
S444から
S412から
S446
貸出フラグ
可？
No
Yes
S448
指定されたエントリ内の貸出フラグを貸出中に変更し、
受理したライセンスIDを貸出ライセンスIDフィールドに
受理したKPmc4を貸出先IDフィールドへ格納
S450
貸出用ACm〔move_cnt=移動・複製禁止〕の生成し
受理したライセンスIDと生成したACmを
指定されたエントリから取得したライセンスID、ACmと置換
S452
ライセンス（ライセンスID、コンテンツID、Kc、ACmおよびACp）
をKmc4にて暗号化し、
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成
S454
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を
Ks2bにて暗号化し、
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの出力
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2b
を貸出元から受理し、貸出先に入力
S456
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2b
の入力を受けてKs2bにて復号
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4の受理
S458
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4
をKmc4にて復号
ライセンスID、コンテンツID、Kc、ACmおよびACpの受理
S460
貸出先ライセンス管理情報から
ライセンスを格納するためのエントリ番号を
決定し、貸出先に入力
貸出ライセンス管理情報の更新
S462
貸出
不可
ACmの
確認
S464
貸出
可
ライセンス領域の指定された
エントリ内の貸出フラグを
"可"に設定
S466
S468
ライセンス領域の指定された
エントリ内の貸出フラグを
"不可"に設定
S474
貸出
可
移動or複製？
S476
貸出先ライセンス管理情報に
貸出用ライセンスIDを追記
貸出先ライセンス管理情報の
更新
S470
ライセンス領域の指定された
エントリ内の有効フラグを
"有効"に設定
ライセンス領域の指示されたエントリに
ライセンスID、コンテンツID、Kc、ACm
およびACpを格納
S472
終了
S478

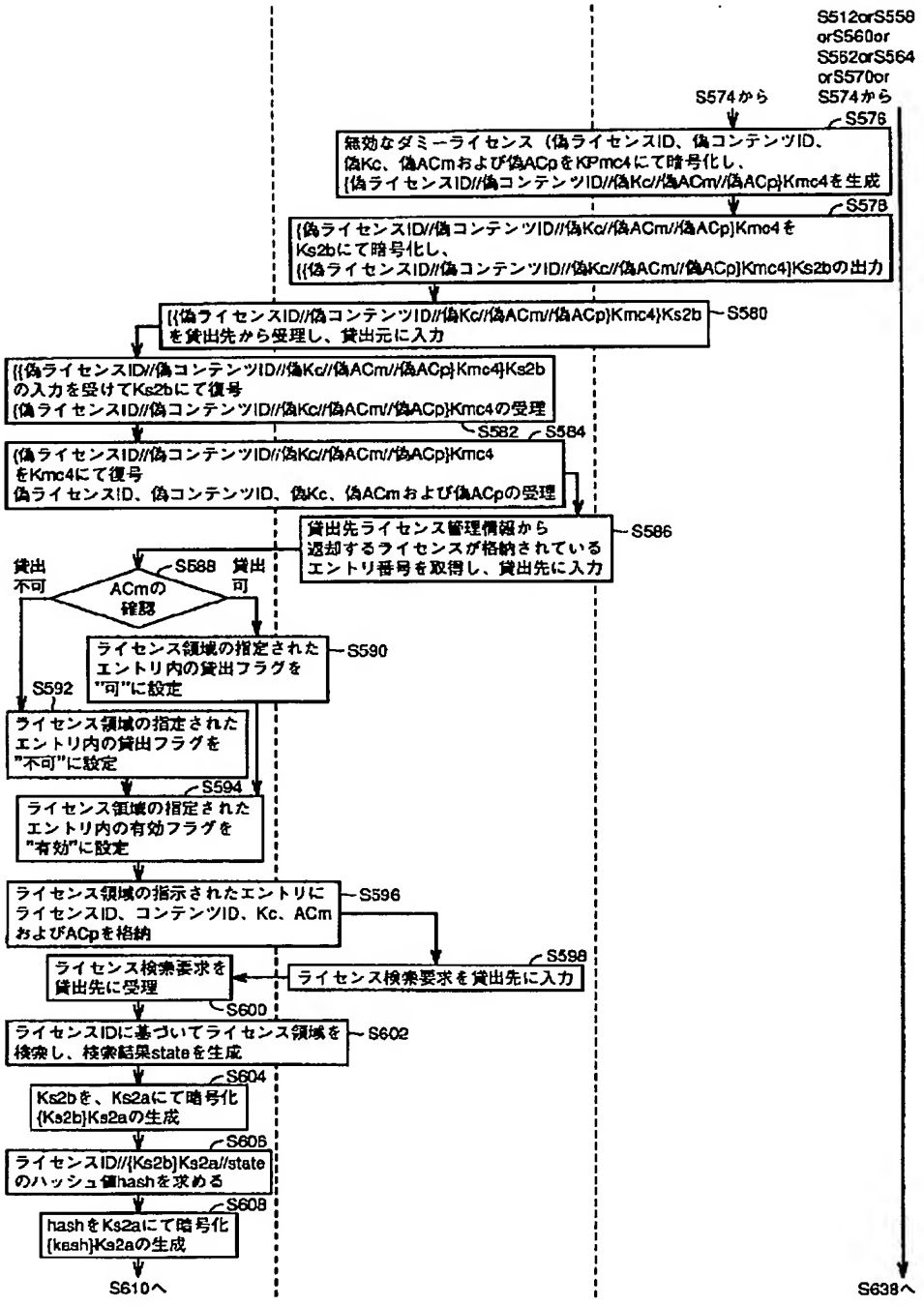
【図１８】


貸出先側
メモリカード110
コントローラ510
貸出元側
ライセンス管理デバイス520
開始
返却リクエスト
S500
S502
貸出先へ認証データ出力要求
S504
認証データ送信要求の受信
S506
{KPm3//Cm3}KPaを出力
{KPm3//Cm3}KPaを
貸出先から受理し、貸出元に入力
S508
S510
{KPm3//Cm3}KPaを受理し
KPaにて復号
S512
KPm3の
受理
No
Yes
S514
セッション鍵Ks2aの生成
S516
Ks2aをKPm3にて暗号化し、
{Ks2a}Km3の出力
S518
{Ks2a}Km3を貸出先から受理
S520
貸出元のライセンス管理情報から
貸出時のライセンスIDを取得
S522
ライセンスID//{Ks2a}Km3
を貸出先に入力
S524
ライセンスID//{Ks2a}Km3
の受理
S526
{Ks2a}Km3をKm3にて復号し、
Ks2aの受理
S528
セッション鍵Ks2bの生成
S530
Ks2bとKPmc4をKs2aにて
暗号化し、
{Ks2b//KPmc4}Ks2aを出力
S532
{Ks2b//KPmc4}Ks2a
を貸出先から受理し、貸出元へ入力
S534
{Ks2b//KPmc4}Ks2a
の入力を受けてKs2aにて復号
Ks2bおよびKPmc4の受理
S534
ライセンス検索要求を貸出先に入力
S535
ライセンス検索要求を受理
S538
ライセンスIDに基づいて
ライセンス領域を検索し、
検索結果stateを生成
S540
Ks2bを、Ks2aにて暗号化
{Ks2b}Ks2aの生成
S542
ライセンスID//{Ks2b}Ks2a//state
のハッシュ値hashを求める
S544
hashをKs2aにて暗号化
{kash}Ks2aの生成
S546へ
S638へ

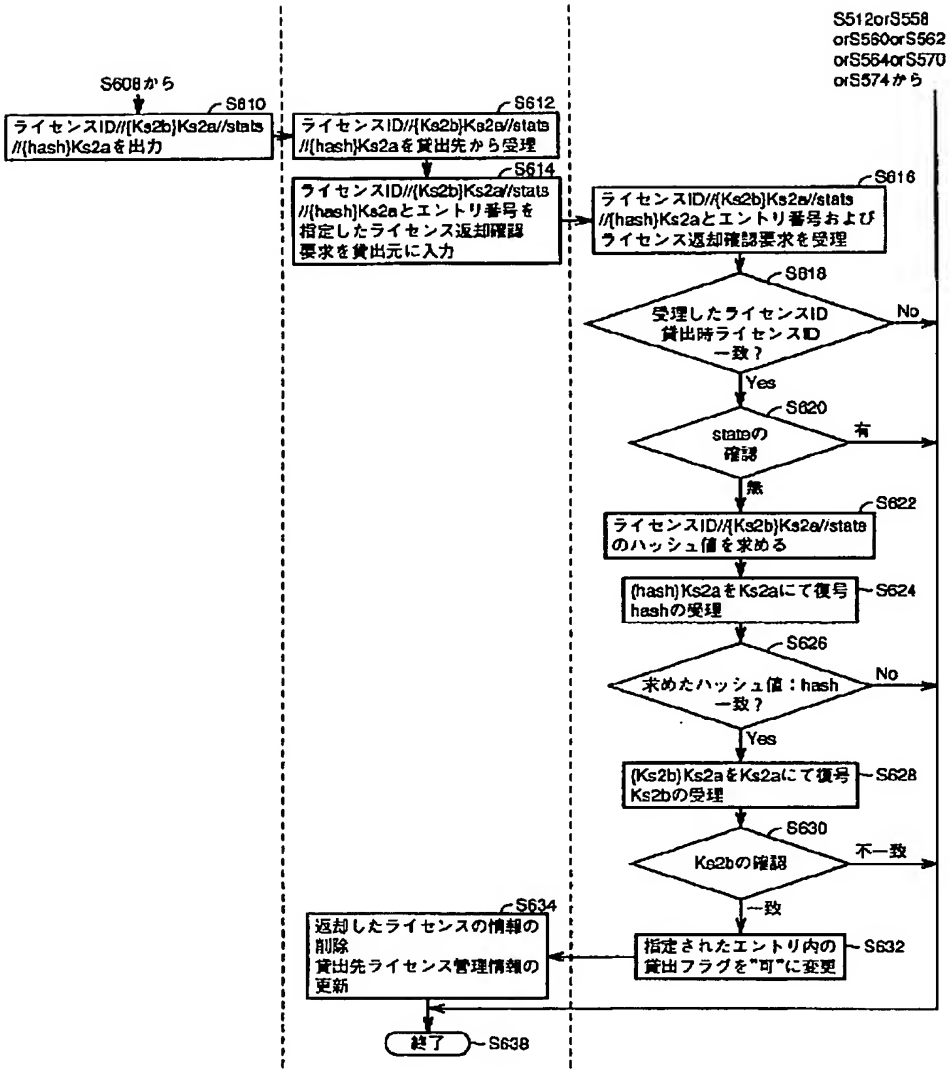
【図１９】


S544から
S546
ライセンスID//{Ks2b}Ks2a//state //{hash}Ks2aを出力
S548
ライセンスID//{Ks2b}Ks2a//state //{hash}Ks2aを貸出先から受理
S550
貸出元のライセンス管理情報から返却するライセンスの格納されているエントリ番号を取得
S552
ライセンスID//{Ks2b}Ks2a//state //{hash}Ks2aとエントリ番号を指定したライセンス返却要求を貸出元に入力
S512から
S554
ライセンスID//{Ks2b}Ks2a//state //{hash}Ks2aとエントリ番号およびライセンス返却要求を受理
S556
指定されたエントリ内の貸出フラグ、貸出時のライセンスIDおよび貸出先IDであるKPmcxを取得
S558
KPmc4：KPmcx 一致？
No
Yes
S560
貸出フラグ 貸出中？
No
Yes
S562
受理したライセンスID 貸出時ライセンスID 一致？
No
Yes
S564
stateの確認
無
有
S566
ライセンスID//{Ks2b}Ks2a//state のハッシュ値を求める
{hash}Ks2aをKs2aにて復号 hashの受理
S568
S570
求めたハッシュ値：hash 一致？
No
Yes
{Ks2b}Ks2aをKs2aにて復号 Ks2bの受理
S572
S574
Ks2bの確認
不一致
一致
S576へ
S638へ

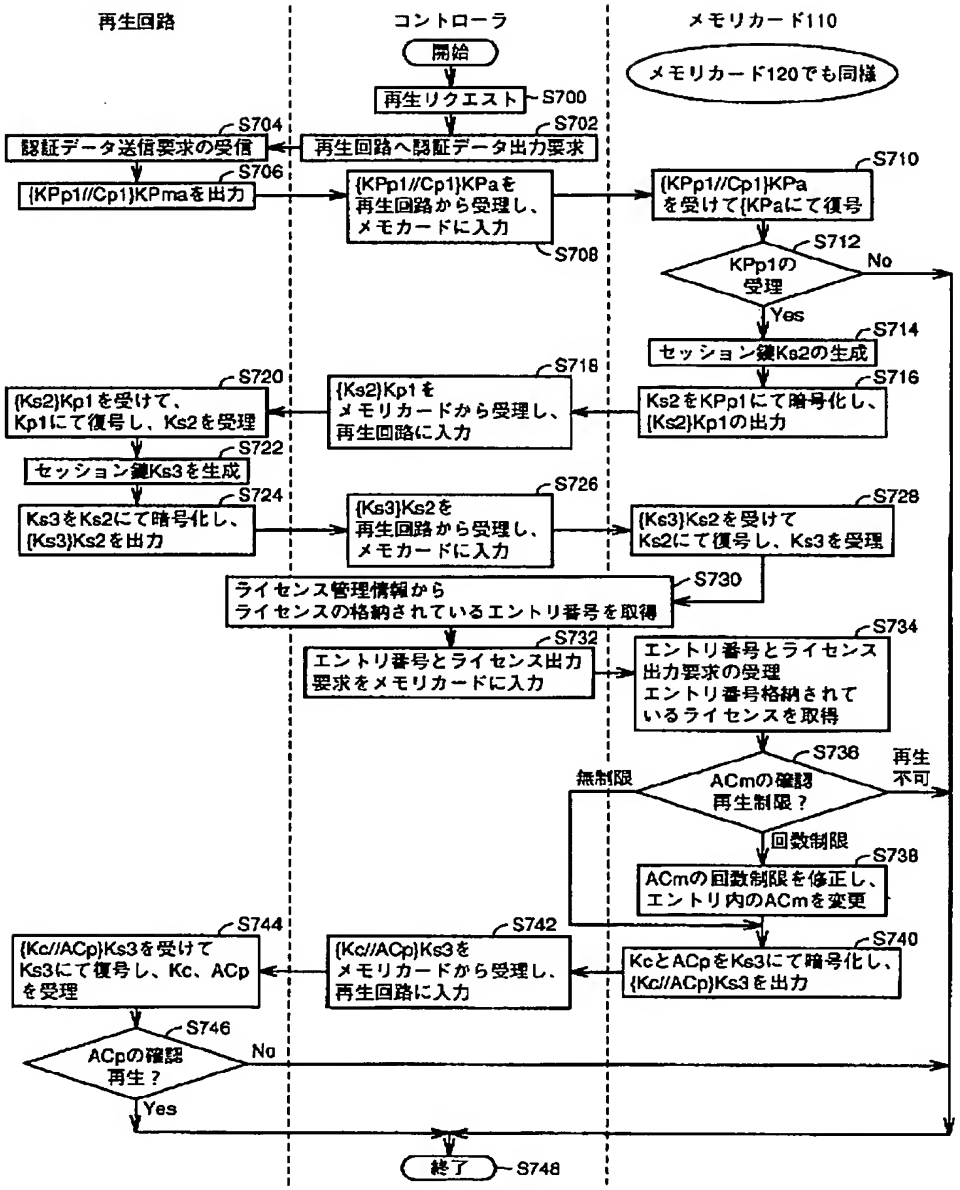
【図２０】


S512orS558
orS560or
S562orS564
orS570or
S574から
S574から
S576
無効なダミーライセンス（偽ライセンスID、偽コンテンツID、
偽Kc、偽ACmおよび偽ACpをKPmc4にて暗号化し、
{偽ライセンスID//偽コンテンツID//偽Kc//偽ACm//偽ACp}Kmc4を生成
S578
{偽ライセンスID//偽コンテンツID//偽Kc//偽ACm//偽ACp}Kmc4を
Ks2bにて暗号化し、
{{偽ライセンスID//偽コンテンツID//偽Kc//偽ACm//偽ACp}Kmc4}Ks2bの出力
{{偽ライセンスID//偽コンテンツID//偽Kc//偽ACm//偽ACp}Kmc4}Ks2b
を貸出先から受理し、貸出元に入力
S580
{{偽ライセンスID//偽コンテンツID//偽Kc//偽ACm//偽ACp}Kmc4}Ks2b
の入力を受けてKs2bにて復号
{偽ライセンスID//偽コンテンツID//偽Kc//偽ACm//偽ACp}Kmc4の受理
S582
S584
{偽ライセンスID//偽コンテンツID//偽Kc//偽ACm//偽ACp}Kmc4
をKmc4にて復号
偽ライセンスID、偽コンテンツID、偽Kc、偽ACmおよび偽ACpの受理
貸出先ライセンス管理情報から
返却するライセンスが格納されている
エントリ番号を取得し、貸出先に入力
S586
貸出
不可
S588
ACmの
確認
貸出
可
ライセンス領域の指定された
エントリ内の貸出フラグを
"可"に設定
S590
S592
ライセンス領域の指定された
エントリ内の貸出フラグを
"不可"に設定
S594
ライセンス領域の指定された
エントリ内の有効フラグを
"有効"に設定
ライセンス領域の指示されたエントリに
ライセンスID、コンテンツID、Kc、ACm
およびACpを格納
S596
ライセンス検索要求を
貸出先に受理
S598
ライセンス検索要求を貸出先に入力
S600
ライセンスIDに基づいてライセンス領域を
検索し、検索結果stateを生成
S602
S604
Ks2bを、Ks2aにて暗号化
{Ks2b}Ks2aの生成
S606
ライセンスID//{Ks2b}Ks2a//state
のハッシュ値hashを求める
S608
hashをKs2aにて暗号化
{kash}Ks2aの生成
S610へ
S638へ

【図２１】


S608から
S610
ライセンスID//{Ks2b}Ks2a//stats //{hash}Ks2aを出力
S612
ライセンスID//{Ks2b}Ks2a//stats //{hash}Ks2aを貸出先から受理
S614
ライセンスID//{Ks2b}Ks2a//stats //{hash}Ks2aとエントリ番号を指定したライセンス返却確認要求を貸出元に入力
S512orS558 orS560orS562 orS564orS570 orS574から
S616
ライセンスID//{Ks2b}Ks2a//stats //{hash}Ks2aとエントリ番号および ライセンス返却確認要求を受理
S618
受理したライセンスID 貸出時ライセンスID 一致？
No
Yes
S620
stateの 確認
有
無
S622
ライセンスID//{Ks2b}Ks2a//stats のハッシュ値を求める
{hash}Ks2aをKs2aにて復号 hashの受理
S624
S626
求めたハッシュ値：hash 一致？
No
Yes
{Ks2b}Ks2aをKs2aにて復号 Ks2bの受理
S628
S630
Ks2bの確認
不一致
一致
S632
指定されたエントリ内の 貸出フラグを"可"に変更
S634
返却したライセンスの情報の 削除
貸出先ライセンス管理情報の 更新
終了
S638

【図２４】




---

フロントページの続き

| (51) Int.Cl.[7] | 識別記号 | F I | ﾃｰﾏｺｰﾄﾞ（参考） |
|---|---|---|---|
| Ｇ０６Ｋ　19/07 | | Ｇ０６Ｋ　19/00 | Ｎ |